

Hooking

Hook

API

Debugging

API Hook

API

SSDT Hooking

IAT Hooking

Hooking

SSDT Hooking

PatchGuard

SSDT Hooking

IAT Hooking

PE

IAT

IAT

Win32 API

NTAPI

IAT

API

calc

PE Bear

IAT

IAT

INT

calc

IAT

PE-bear v0.6.5.2 [C:/Users/Administrator/Desktop/VTF/poc/peshellcodify/calc.exe]

File Settings View Compare Info

calc.exe

DOS Header

DOS stub

NT Headers

Signature

File Header

Optional Header

Section Headers

Sections

.text

EP = C70

.rdata

.data

.pdata

.rsrc

.reloc

0 1 2 3 4 5 6 7 8 9 A B C D E F

C4 29 00 00 00 00 00 00 DA 29 00 00 00 00 00 00

F4 29 00 00 00 00 00 00 04 2A 00 00 00 00 00 00

AE 29 00 00 00 00 00 00 32 2A 00 00 00 00 00 00

46 2A 00 00 00 00 00 00 62 2A 00 00 00 00 00 00

80 2A 00 00 00 00 00 00 94 2A 00 00 00 00 00 00

94 29 00 00 00 00 00 18 2A 00 00 00 00 00 00

00 00 00 00 00 00 00 78 29 00 00 00 00 00 00

00 00 00 00 00 00 00 FC 2B 00 00 00 00 00 00

0 1 2 3 4 5 6 7 8 9 A B C D E F

Ä) Û)

ö) *

©) 2 *

F * b *

. * *

) *

. x)

. i +

Disasm: .rdata

General

DOS Hdr

Rich Hdr

File Hdr

Optional Hdr

Section Hdrs

Imports

Resources

Exception

BaseReloc.

Offset	Name	Func. Count	Bound?	OriginalFirstThunk	TimeDateStamp	Forwarder	NameRVA	FirstThunk
1794	SHELL32.dll	1	FALSE	28C0	0	0	2988	21B0
17A8	KERNEL32.dll	12	FALSE	2858	0	0	2AA8	2148
17BC	msvcrt.dll	14	FALSE	2900	0	0	2B68	21F0
17D0	ADVAPI32.dll	3	FALSE	2838	0	0	2BC4	2128
17E4	api-ms-win-core-sync...	1	FALSE	28F0	0	0	2C00	21E0
17F8	api-ms-win-core-proc...	1	FALSE	28E0	0	0	2C22	21D0
180C	api-ms-win-core-libra...	1	FALSE	28D0	0	0	2C4C	21C0

KERNEL32.dll [12 entries]

Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder	Hint
2148	GetCurrentThreadId	-	29C4	29C4	-	224
2150	GetSystemTimeAsFileTime	-	29DA	29DA	-	2F2
2158	GetTickCount	-	29F4	29F4	-	310
2160	RtlCaptureContext	-	2A04	2A04	-	4D4
2168	GetCurrentProcessId	-	29AE	29AE	-	220
2170	RtlVirtualUnwind	-	2A32	2A32	-	4E2
2178	UnhandledExceptionFilter	-	2A46	2A46	-	5BE
2180	SetUnhandledExceptionFilter	-	2A62	2A62	-	57D
2188	GetCurrentProcess	-	2A80	2A80	-	21F

WinDBG

```
0:000> dq 00007FF7DB832148
00007ff7`db832148 00007fff`4bad5860 00007fff`4bad7e90
00007ff7`db832158 00007fff`4bad5950 00007fff`4bae49d0
00007ff7`db832168 00007fff`4bae4ba0 00007fff`4bac1010
00007ff7`db832178 00007fff`4bafba90 00007fff`4bae0110
00007ff7`db832188 00007fff`4bae4b90 00007fff`4bae0a70
00007ff7`db832198 00007fff`4bad5f20 00007fff`4badd600
00007ff7`db8321a8 00000000`00000000 00007fff`4b129040
00007ff7`db8321b8 00000000`00000000 00007fff`4995e730
0:000> u 00007fff`4bad5860 l1
KERNEL32!GetCurrentThreadId:
00007fff`4bad5860 65488b042530000000 mov     rax,qword ptr gs:[30h]
```

IAT

IAT Hooking

EDR

Hooking

Hooking

Hooking

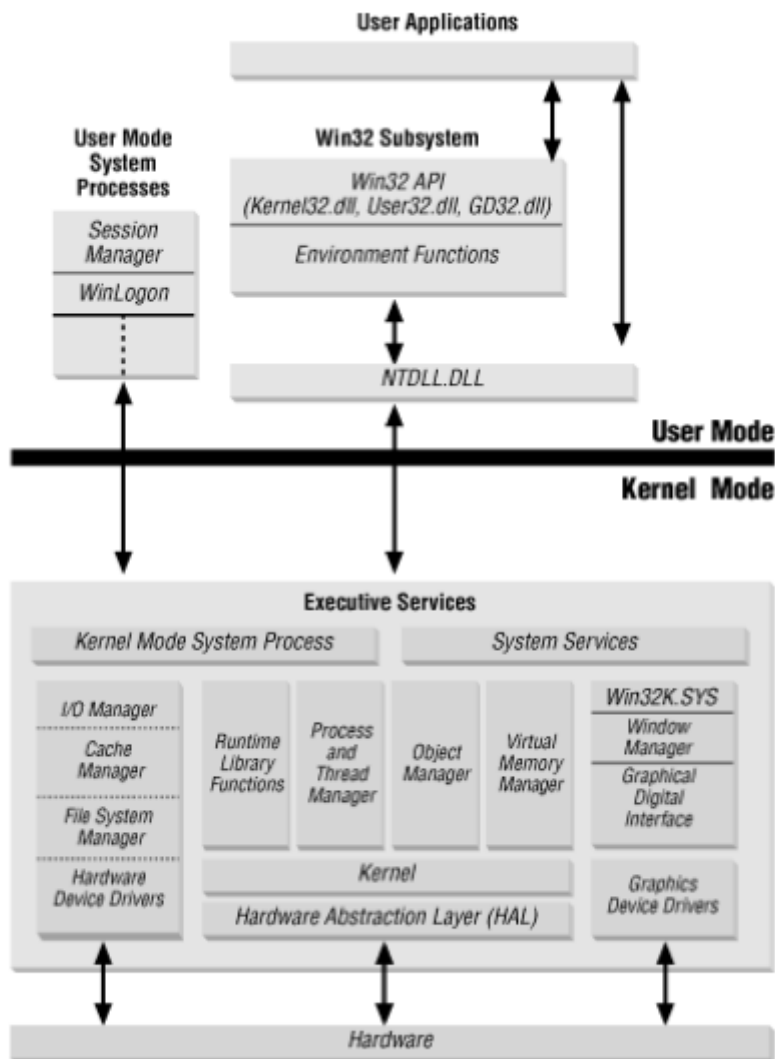
EDR

NTAPI

Hook **system! jmp**

Hook

NTAPI



NtWriteVirtualMemory Win32 API **WriteProcessMemory** 2 hook
) hook **mov r10, rcx** syscall syscall

```

ntdll!NtWriteVirtualMemory:
00007ff9`1748faa0 4c8bd1      mov     r10,rcx
00007ff9`1748faa3 e9c6f30800  jmp     ntdll!StartPathWithLongPathPrefixIfNeeded+0xcae (00007ff9`1751ee6e)
00007ff9`1748faa8 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007ff9`1748fab0 7503        jne     ntdll!NtWriteVirtualMemory+0x15 (00007ff9`1748fab5)
00007ff9`1748fab2 0f05        syscall
00007ff9`1748fab4 c3          ret
00007ff9`1748fab5 cd2e        int     2Eh
00007ff9`1748fab7 c3          ret
00007ff9`1748fab8 0f1f840000000000 nop     dword ptr [rax+rax]
  
```

NTAPI hook

```

0:000> u ntdll!NtDrawText
ntdll!NtDrawText:
00007ff9`17490fb0 4c8bd1      mov     r10,rcx
00007ff9`17490fb3 b8e3000000 mov     eax,0E3h
00007ff9`17490fb8 f604250803fe7f01 test    byte ptr [SharedUserData+0x308 (00000000`7ffe0308)],1
00007ff9`17490fc0 7503        jne     ntdll!NtDrawText+0x15 (00007ff9`17490fc5)
00007ff9`17490fc2 0f05        syscall
00007ff9`17490fc4 c3          ret
00007ff9`17490fc5 cd2e        int     2Eh
00007ff9`17490fc7 c3          ret
  
```

NTAPI

syscall

x64

syscall

```
mov r10, rcx  
mov rax, [SSN]  
syscall  
ret
```

Hook

Revision #7

Created 1 June 2023 03:10:55 by

Updated 1 April 2024 00:02:06 by unknown