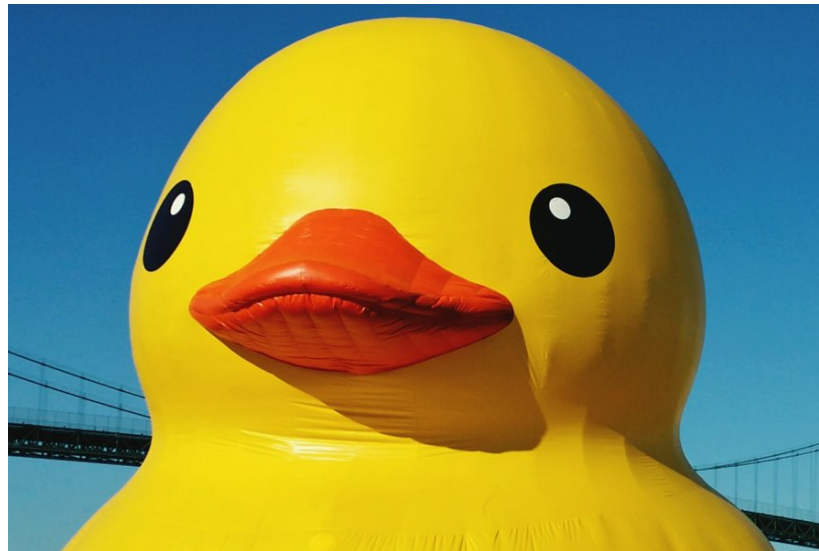


SmokeLoader Analysis

Kent Pang

Iamwho <

- Collector of random Sh*t
- Owner of the domain go-outside.xyz
- Malware reversing hobbyist



SmokeLoader

- A loader type malware
- Highly obfuscated
- Extremely common

The image displays two screenshots of the SmokeLoader web interface, which is used for managing a botnet.

Left Screenshot: MY BOTNET Dashboard

- MY BOTNET** sidebar menu: BOT LIST, TASK LIST, OPTIONS, STEALER, PROCMON, FAKE DNS.
- STATISTIC** table:

STATISTIC	OS	PRIVILEGES	SELLERS	ONLINE SELLERS	ONLINE COUNTRIES	COUNTRIES
ALL BOTS - 3580	WINDOWS 10 - 1730	LOW - 0	- 3580	- 319	SHOW/HIDE	SHOW/HIDE
TODAY - 1509	WINDOWS 7 - 1370	MEDIUM+ - 3580				
ONLINE - 319	WINDOWS 11 - 324					
TASKS - 1	WINDOWS 8.1 - 123					
LOADS - 1015	WINDOWS 8 - 32					
RUNS - 958	OTHER - 1					
UPDATING - 0						
INSTALLED - 3140						
- LAST BOTS** table:

LAST BOTS
SHOW/HIDE
- SERVER** information: DATE: 11.11.2022, TIME: 16:20:40, PHP: [REDACTED], MYSQL: [REDACTED].

Right Screenshot: ADD NEW TASK Form

- TASK LIST** table:

ID	SIZE	DATE	LOADS	RUNS	ACTION	LIMIT	URL	GEO	RUN TYPE	BITS	DELETE BOT	COMMENT	SELLER	GUEST
1	6 KB	11.11.2022 03:36:22	1020	963	DELETE EDIT STOP	0	LOCAL	LOCAL	RUNEXE	X32 & X64	NO	[REDACTED]	0	LINK
- ADD NEW TASK** form:
 - LOCAL FILE** and **REMOTE FILE** sections.
 - COMMENT:** [Text input]
 - GEO:** [Dropdown menu, currently set to ALL]
 - LIMIT:** [Input field, value 0]
 - SELLER:** [Input field, value 0]
 - OPTIONS:** RUNEXE (selected), LOADDLL, REGSVR32, RUNMEM, RUNBAT, X32 & X64 (selected), X32, X64, DELETE BOT AFTER COMPLETE TASKS (checkbox).

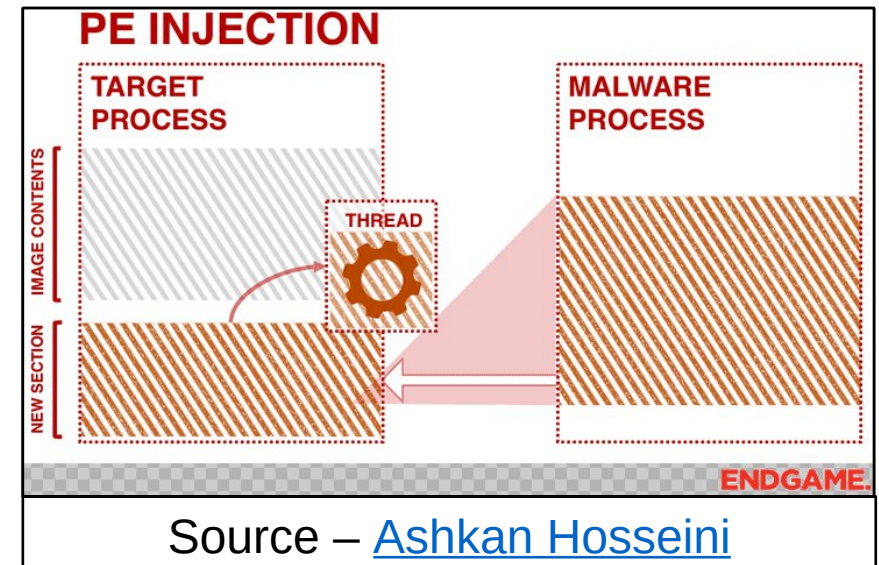
Source: [VxUnderground's](#) twitter

Stage 1

Pre-Smoked

What is Process Injection

- Injecting code onto itself or into other processes and having the code run
- Generally performed with WinApis
- Generic Process Injection APIs
 - VirtualAlloc
 - VirtualProtect
 - WriteProcessMemory
 - CreateProcessInternalW



Dumping Packed Payload

- Dumping Payload with VirtualAlloc()
- Self-Injection type injection
- Decrypts encrypted PE
- Writes it to empty section
- Jumps to new location and executes PE

property	value
general	
name	.bss
md5	n/a
entropy	n/a
file-ratio (96.33%)	n/a
raw-address	0x00022200
raw-size (233984 bytes)	0x00000000 (0 bytes)
virtual-address	0x00024000
virtual-size (240340 bytes)	0x00001000 (4096 bytes)

The screenshot shows a debugger window with assembly code on the left and a memory dump on the right. The assembly code is for a function named `VirtualAlloc`. The code starts with `mov edi,edi`, `push ebp`, `mov ebp,esp`, and `pop ebp`. It then jumps to a new location `JMP.&VirtualAlloc`. The memory dump shows the raw data of the payload, which is a PE file. The dump is organized into columns for address, hex, and ASCII. The ASCII column shows the 'MZ' magic number, indicating it's a PE file. The dump also shows the 'PE' signature and the 'ntoskrnl.exe' name.

```
75DEF9F0 8BFF mov edi,edi
75DEF9F2 55 push ebp
75DEF9F3 8BEC mov ebp,esp
75DEF9F5 5D pop ebp
75DEF9F6 FF25 6C13E575 jmp dword ptr ds:[<&VirtualAlloc>]
75DEF9FC CC int3
75DEF9FD CC int3
75DEF9FE CC int3
75DEF9FF CC int3
75DEFA00 CC int3
75DEFA01 CC int3
75DEFA02 CC int3
75DEFA03 CC int3
75DEFA04 CC int3
75DEFA05 CC int3
75DEFA06 CC int3
75DEFA07 CC int3
```

edi=200 L'Ä'

.text:75DEF9F0 kernel32.dll:1F9F0 #109F0 <VirtualAlloc>

Address	Hex	ASCII
00BA0000	4D 5A 80 00 01 00 00 00 04 00 10 00 FF FF 00 00	MZ.....ÿÿ..
00BA0010	40 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00	@.....@.....
00BA0020	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00BA0030	00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00	
00BA0040	0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68	!..Li!Th
00BA0050	69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F	is program canno

Stage 2

Pain.jpeg

Obfuscation Techniques

Aka funny text make life hard

Anti-Analysis

- TEB & PEB
 - Thread Environment Block & Process Environment Block
 - What Is TEB & PEB?
 - ISDebugged? 0x30 -> 0x02
 - NTGlobal Flag? 0x30 -> 0x68
- Avoids the need to call APIs

PEB structure (winternl.h)

Article • 09/01/2022 • 2 minutes to read

[Feedback](#)

[This structure may be altered in future versions of Windows.]

Contains process information.

2.2. NtGlobalFlag

The `NtGlobalFlag` field of the Process Environment Block (0x68 offset on 32-Bit and 0xBC on 64-bit Windows) is 0 by default. Attaching a debugger doesn't change the value of `NtGlobalFlag`. However, if the process was created by a debugger, the following flags will be set:

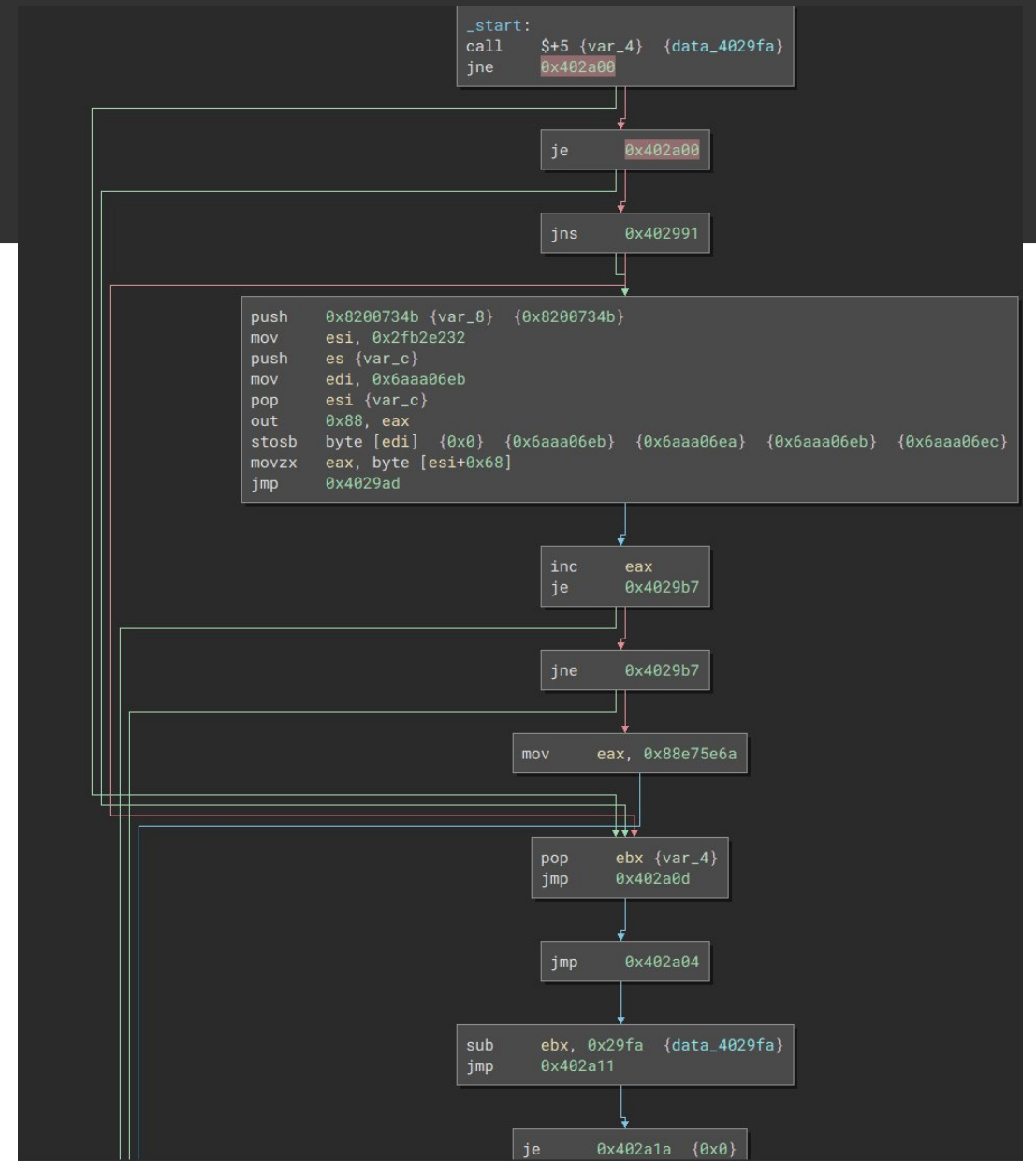
- `FLG_HEAP_ENABLE_TAIL_CHECK` (0x10)
- `FLG_HEAP_ENABLE_FREE_CHECK` (0x20)
- `FLG_HEAP_VALIDATE_PARAMETERS` (0x40)

The presence of a debugger can be detected by checking a combination of those flags.

[CheckPoint's AntiDebug List](#)

Opaque Predicates

- Multiple conditional Jump instructions
- Obfuscates control flow
- Makes static analysis not fun
- Cheeky NtGlobalFlag



SandBox & AV Detection

- Looks for 3 DLLs and if found, the process will exit
 - Sandboxie
 - slbiedll.dll
 - AVG AntiVirus
 - Aswhook.dll
 - Avast AntiVirus
 - snxhk.dll

LdrGetDllHandle	FileName: sbiedll ModuleHandle: 0xfffffffffe00fe00	failed
LdrGetDllHandle	FileName: aswhook ModuleHandle: 0x7721e355	failed
LdrGetDllHandle	FileName: snxhk ModuleHandle: 0x7721e355	failed

- Checks HKLM\CurrentControlSet\Enum\IDE & SCSI

- QEMU
- VBOX
- VIRTIO
- VMWARE
- XEN

Varsity
College

Propagate Injection

Malicious code go brrrr

Propagate Injection

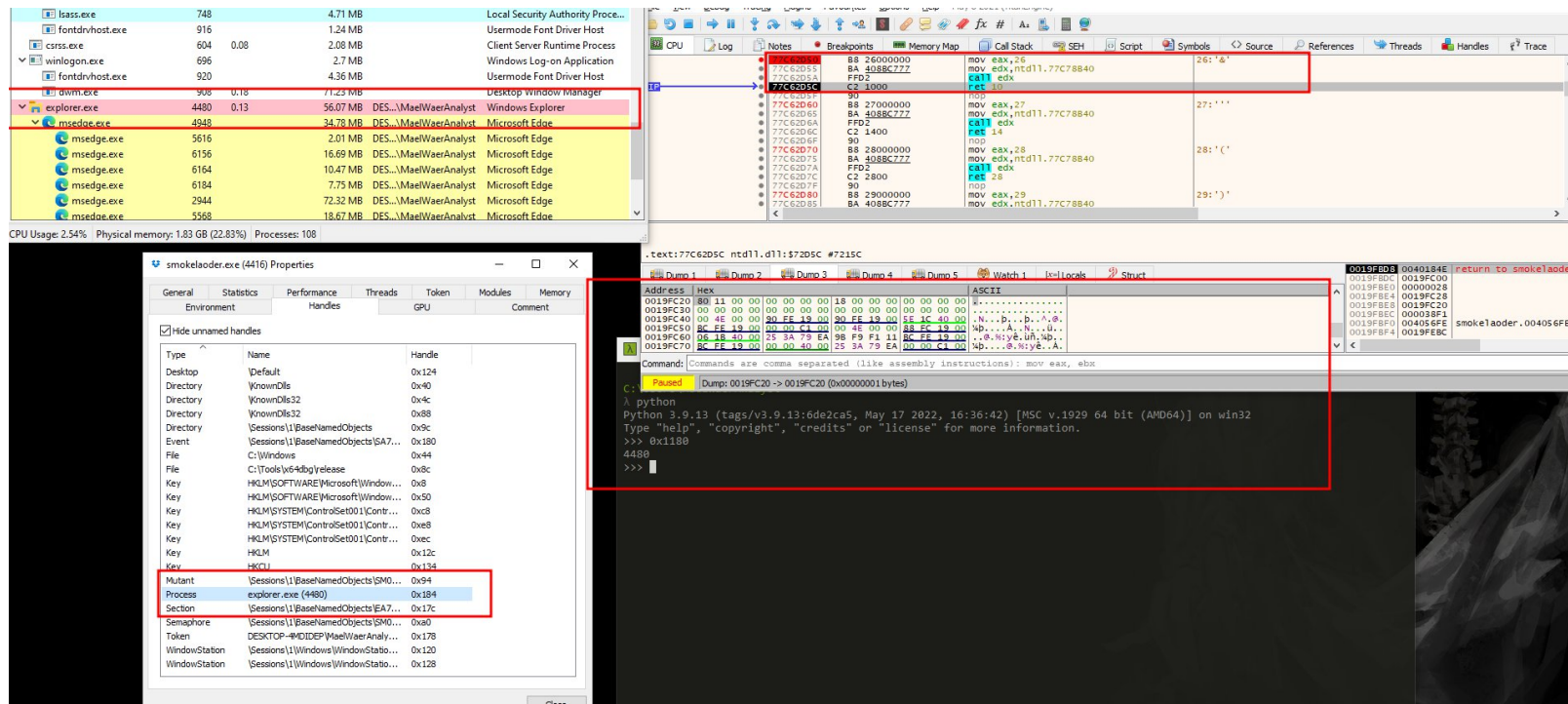
- Stealthy
- Doesn't spawn external processes
- Performed by exploiting Window's UxSubClassesInfo property
- Can really only be used to inject and execute shellcode

SmokeLoader Propagate Injection APIs

- NtOpenProcess()
- ZwCreateSection()
- NtMapViewOfSection()
- ZwUnmapViewOfSection()
- EnumPropA()
- SetPropA()
- SendMessageA()
- SendNotifyMessageA()

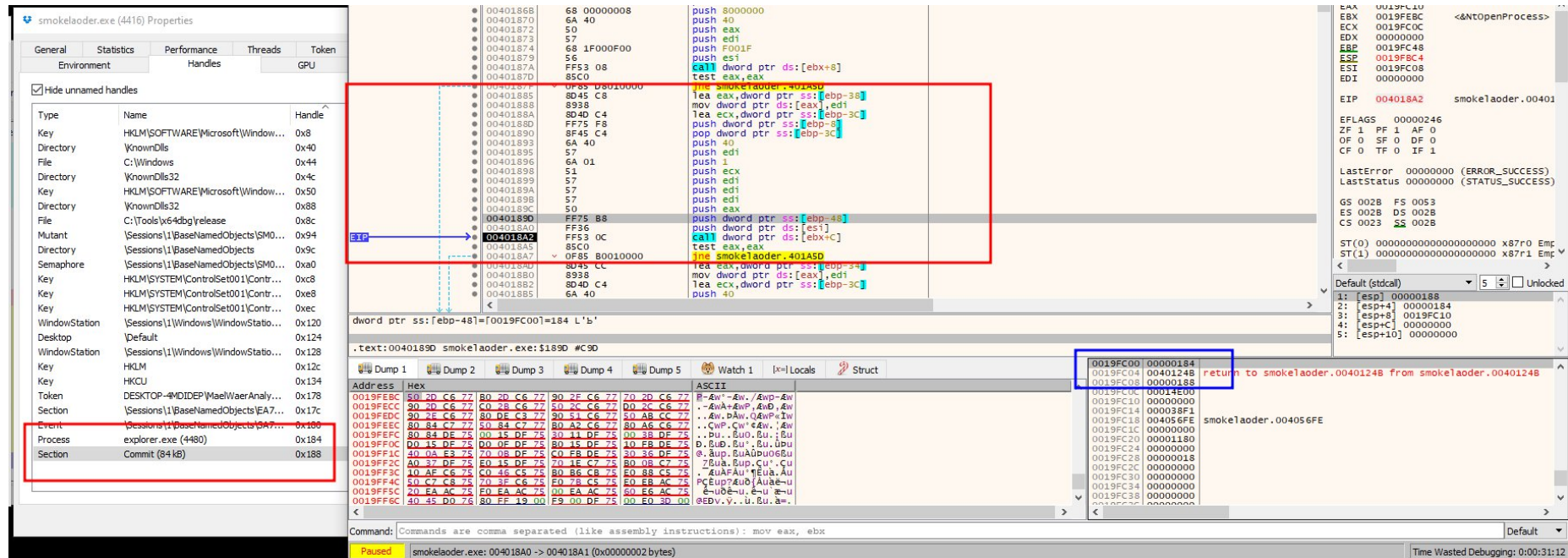
NtOpenProcess()

- The parent process creates an handle explorer.exe
- Allows the parent process to retrieve and manipulate the handled process



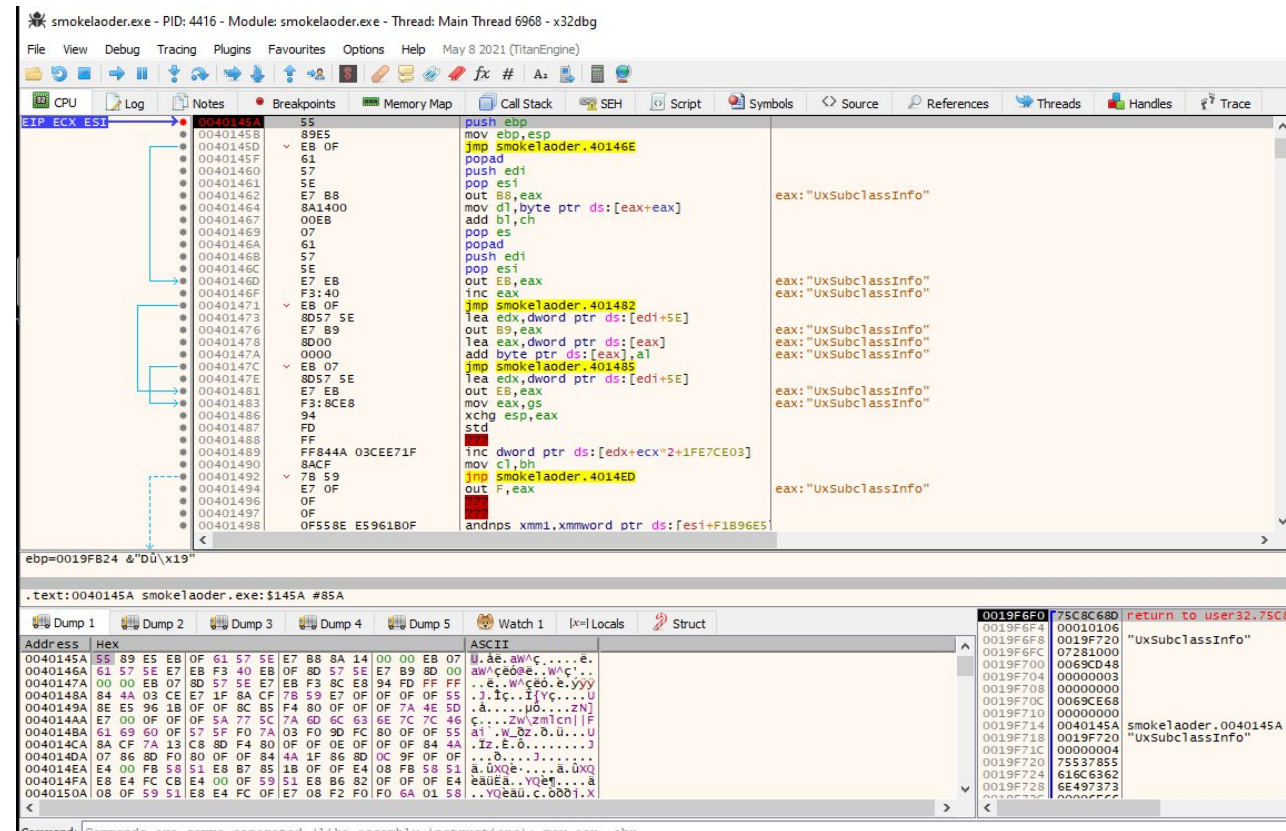
Mapping Memory Space

- Uses ZwCreateSection and ZwMapSection to allocate memory space into explorer.exe



Locating UxSubClassInfo

- EnumsPropA
 - Checks Explorer.exe if the property UxSubClassInfo is present



The screenshot displays a debugger window for the process 'smokelaoder.exe' (PID: 4416). The assembly view shows the following instructions:

```
0040145A 55          push ebp
0040145B 89E5        mov ebp,esp
0040145D E8 0F       jmp smokelaoder.40146E
0040145F 61          popad
00401460 57          push edi
00401461 5E          pop esi
00401462 E7 B8       out B8,eax
00401464 8A1400      mov dl,byte ptr ds:[eax+eax]
00401467 00EB       add bl,ch
00401469 07          pop es
0040146A 61          popad
0040146B 57          push edi
0040146C 5E          pop esi
0040146D E7 E8       out E8,eax
0040146F F3 40      inc eax
00401471 E8 0F       jmp smokelaoder.401482
00401473 8D57 5E     lea edx,dword ptr ds:[edi+5E]
00401476 E7 B9       out B9,eax
00401478 8D00      lea eax,dword ptr ds:[eax]
0040147A 0000      add byte ptr ds:[eax],al
0040147C E8 07       jmp smokelaoder.401485
0040147E 8D57 5E     lea edx,dword ptr ds:[edi+5E]
00401481 E7 E8       out E8,eax
00401483 F3 40      mov eax,gs
00401486 94          xchg esp,eax
00401487 FD          std
00401488 FF          inc dword ptr ds:[edx+ecx*2+1FE7CE03]
00401489 8ACF       mov cl,bh
00401492 7B 59      jmp smokelaoder.4014ED
00401494 E7 0F       out F,eax
00401496 0F         andnps xmm1,xmmword ptr ds:[esi+F1B9E5]
00401498 0F558E E5961B0F andnps xmm1,xmmword ptr ds:[esi+F1B9E5]
```

The dump view at the bottom shows the following memory addresses and hex values:

Address	Hex
0040145A	55 89 E5 EB 0F 61 57 5E E7 B8 8A 14 00 00 E8 07
0040145B	89 E5 EB F3 40 E8 0F 8D 57 5E E7 B9 8D 00
0040145D	61 57 5E E7 E8 F3 8C E8 94 FD FF FF
0040145F	00 00 E8 07 8D 57 5E E7 E8 F3 8C E8 94 FD FF FF
00401460	57 5E E7 8D 57 5E E7 E8 F3 8C E8 94 FD FF FF
00401461	5E 8D 57 5E E7 8D 57 5E E7 E8 F3 8C E8 94 FD FF FF
00401462	8A 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401463	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401464	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401465	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401466	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401467	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401468	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401469	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040146F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401470	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401471	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401472	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401473	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401474	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401475	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401476	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401477	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401478	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401479	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040147F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401480	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401481	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401482	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401483	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401484	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401485	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401486	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401487	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401488	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401489	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148A	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148B	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148D	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040148F	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401490	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401491	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401492	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401493	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401494	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401495	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401496	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401497	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00401498	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Struct Injection

- Injects the malicious UxSubClassInfo structure
- Follows the previous injection technique with ZwCreateSection & ZwMapSection

The screenshot displays a debugger interface with two main panes. The top pane shows assembly code with addresses, hex values, and disassembled instructions. The bottom pane shows a memory dump with addresses, hex values, and ASCII representations.

Assembly Code:

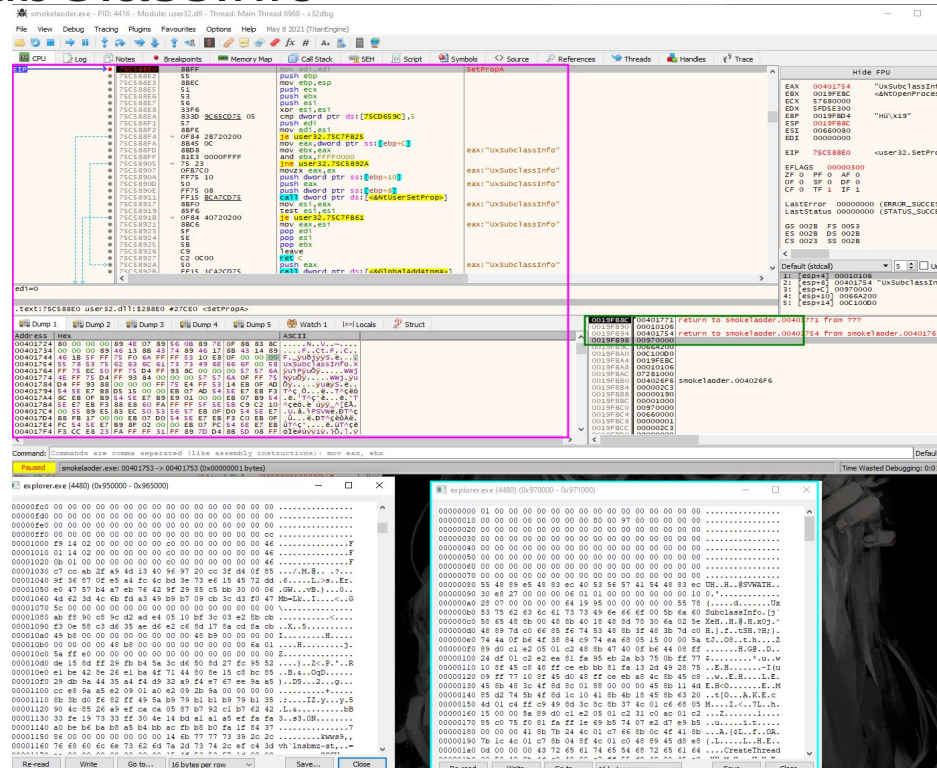
```
00401000 mov eax, 2A
00401001 mov edx, ntdll.77C78B40
00401002 call edx
00401003 mov eax, 2B
00401004 mov edx, ntdll.77C78B40
00401005 call edx
00401006 mov eax, 7002C
00401007 mov edx, ntdll.77C78B40
00401008 call edx
00401009 mov eax, 3002D
0040100A mov edx, ntdll.77C78B40
0040100B call edx
0040100C mov eax, 1A002E
0040100D mov edx, ntdll.77C78B40
0040100E call edx
0040100F mov eax, 2F
00401010 mov edx, ntdll.77C78B40
00401011 call edx
00401012 mov eax, 30
00401013 mov edx, ntdll.77C78B40
00401014 call edx
00401015 mov eax, 50031
00401016 mov edx, ntdll.77C78B40
00401017 call edx
00401018 mov eax, 32
00401019 mov edx, ntdll.77C78B40
0040101A call edx
0040101B mov eax, 33
0040101C mov edx, ntdll.77C78B40
0040101D call edx
0040101E mov eax, 34
0040101F mov edx, ntdll.77C78B40
00401020 call edx
00401021 mov eax, 35
00401022 mov edx, ntdll.77C78B40
00401023 call edx
00401024 mov eax, 36
00401025 mov edx, ntdll.77C78B40
00401026 call edx
00401027 mov eax, 37
00401028 mov edx, ntdll.77C78B40
00401029 call edx
0040102A mov eax, 38
0040102B mov edx, ntdll.77C78B40
0040102C call edx
0040102D mov eax, 39
0040102E mov edx, ntdll.77C78B40
0040102F call edx
00401030 mov eax, 3A
00401031 mov edx, ntdll.77C78B40
00401032 call edx
00401033 mov eax, 3B
00401034 mov edx, ntdll.77C78B40
00401035 call edx
00401036 mov eax, 3C
00401037 mov edx, ntdll.77C78B40
00401038 call edx
00401039 mov eax, 3D
0040103A mov edx, ntdll.77C78B40
0040103B call edx
0040103C mov eax, 3E
0040103D mov edx, ntdll.77C78B40
0040103E call edx
0040103F mov eax, 3F
00401040 mov edx, ntdll.77C78B40
00401041 call edx
00401042 mov eax, 40
00401043 mov edx, ntdll.77C78B40
00401044 call edx
00401045 mov eax, 41
00401046 mov edx, ntdll.77C78B40
00401047 call edx
00401048 mov eax, 42
00401049 mov edx, ntdll.77C78B40
0040104A call edx
0040104B mov eax, 43
0040104C mov edx, ntdll.77C78B40
0040104D call edx
0040104E mov eax, 44
0040104F mov edx, ntdll.77C78B40
00401050 call edx
00401051 mov eax, 45
00401052 mov edx, ntdll.77C78B40
00401053 call edx
00401054 mov eax, 46
00401055 mov edx, ntdll.77C78B40
00401056 call edx
00401057 mov eax, 47
00401058 mov edx, ntdll.77C78B40
00401059 call edx
0040105A mov eax, 48
0040105B mov edx, ntdll.77C78B40
0040105C call edx
0040105D mov eax, 49
0040105E mov edx, ntdll.77C78B40
0040105F call edx
00401060 mov eax, 4A
00401061 mov edx, ntdll.77C78B40
00401062 call edx
00401063 mov eax, 4B
00401064 mov edx, ntdll.77C78B40
00401065 call edx
00401066 mov eax, 4C
00401067 mov edx, ntdll.77C78B40
00401068 call edx
00401069 mov eax, 4D
0040106A mov edx, ntdll.77C78B40
0040106B call edx
0040106C mov eax, 4E
0040106D mov edx, ntdll.77C78B40
0040106E call edx
0040106F mov eax, 4F
00401070 mov edx, ntdll.77C78B40
00401071 call edx
00401072 mov eax, 50
00401073 mov edx, ntdll.77C78B40
00401074 call edx
00401075 mov eax, 51
00401076 mov edx, ntdll.77C78B40
00401077 call edx
00401078 mov eax, 52
00401079 mov edx, ntdll.77C78B40
0040107A call edx
0040107B mov eax, 53
0040107C mov edx, ntdll.77C78B40
0040107D call edx
0040107E mov eax, 54
0040107F mov edx, ntdll.77C78B40
00401080 call edx
00401081 mov eax, 55
00401082 mov edx, ntdll.77C78B40
00401083 call edx
00401084 mov eax, 56
00401085 mov edx, ntdll.77C78B40
00401086 call edx
00401087 mov eax, 57
00401088 mov edx, ntdll.77C78B40
00401089 call edx
0040108A mov eax, 58
0040108B mov edx, ntdll.77C78B40
0040108C call edx
0040108D mov eax, 59
0040108E mov edx, ntdll.77C78B40
0040108F call edx
00401090 mov eax, 5A
00401091 mov edx, ntdll.77C78B40
00401092 call edx
00401093 mov eax, 5B
00401094 mov edx, ntdll.77C78B40
00401095 call edx
00401096 mov eax, 5C
00401097 mov edx, ntdll.77C78B40
00401098 call edx
00401099 mov eax, 5D
0040109A mov edx, ntdll.77C78B40
0040109B call edx
0040109C mov eax, 5E
0040109D mov edx, ntdll.77C78B40
0040109E call edx
0040109F mov eax, 5F
004010A0 mov edx, ntdll.77C78B40
004010A1 call edx
004010A2 mov eax, 60
004010A3 mov edx, ntdll.77C78B40
004010A4 call edx
004010A5 mov eax, 61
004010A6 mov edx, ntdll.77C78B40
004010A7 call edx
004010A8 mov eax, 62
004010A9 mov edx, ntdll.77C78B40
004010AA call edx
004010AB mov eax, 63
004010AC mov edx, ntdll.77C78B40
004010AD call edx
004010AE mov eax, 64
004010AF mov edx, ntdll.77C78B40
004010B0 call edx
004010B1 mov eax, 65
004010B2 mov edx, ntdll.77C78B40
004010B3 call edx
004010B4 mov eax, 66
004010B5 mov edx, ntdll.77C78B40
004010B6 call edx
004010B7 mov eax, 67
004010B8 mov edx, ntdll.77C78B40
004010B9 call edx
004010BA mov eax, 68
004010BB mov edx, ntdll.77C78B40
004010BC call edx
004010BD mov eax, 69
004010BE mov edx, ntdll.77C78B40
004010BF call edx
004010C0 mov eax, 6A
004010C1 mov edx, ntdll.77C78B40
004010C2 call edx
004010C3 mov eax, 6B
004010C4 mov edx, ntdll.77C78B40
004010C5 call edx
004010C6 mov eax, 6C
004010C7 mov edx, ntdll.77C78B40
004010C8 call edx
004010C9 mov eax, 6D
004010CA mov edx, ntdll.77C78B40
004010CB call edx
004010CC mov eax, 6E
004010CD mov edx, ntdll.77C78B40
004010CE call edx
004010CF mov eax, 6F
004010D0 mov edx, ntdll.77C78B40
004010D1 call edx
004010D2 mov eax, 70
004010D3 mov edx, ntdll.77C78B40
004010D4 call edx
004010D5 mov eax, 71
004010D6 mov edx, ntdll.77C78B40
004010D7 call edx
004010D8 mov eax, 72
004010D9 mov edx, ntdll.77C78B40
004010DA call edx
004010DB mov eax, 73
004010DC mov edx, ntdll.77C78B40
004010DD call edx
004010DE mov eax, 74
004010DF mov edx, ntdll.77C78B40
004010E0 call edx
004010E1 mov eax, 75
004010E2 mov edx, ntdll.77C78B40
004010E3 call edx
004010E4 mov eax, 76
004010E5 mov edx, ntdll.77C78B40
004010E6 call edx
004010E7 mov eax, 77
004010E8 mov edx, ntdll.77C78B40
004010E9 call edx
004010EA mov eax, 78
004010EB mov edx, ntdll.77C78B40
004010EC call edx
004010ED mov eax, 79
004010EE mov edx, ntdll.77C78B40
004010EF call edx
004010F0 mov eax, 7A
004010F1 mov edx, ntdll.77C78B40
004010F2 call edx
004010F3 mov eax, 7B
004010F4 mov edx, ntdll.77C78B40
004010F5 call edx
004010F6 mov eax, 7C
004010F7 mov edx, ntdll.77C78B40
004010F8 call edx
004010F9 mov eax, 7D
004010FA mov edx, ntdll.77C78B40
004010FB call edx
004010FC mov eax, 7E
004010FD mov edx, ntdll.77C78B40
004010FE call edx
004010FF mov eax, 7F
00401100 mov edx, ntdll.77C78B40
00401101 call edx
00401102 mov eax, 80
00401103 mov edx, ntdll.77C78B40
00401104 call edx
00401105 mov eax, 81
00401106 mov edx, ntdll.77C78B40
00401107 call edx
00401108 mov eax, 82
00401109 mov edx, ntdll.77C78B40
0040110A call edx
0040110B mov eax, 83
0040110C mov edx, ntdll.77C78B40
0040110D call edx
0040110E mov eax, 84
0040110F mov edx, ntdll.77C78B40
00401110 call edx
00401111 mov eax, 85
00401112 mov edx, ntdll.77C78B40
00401113 call edx
00401114 mov eax, 86
00401115 mov edx, ntdll.77C78B40
00401116 call edx
00401117 mov eax, 87
00401118 mov edx, ntdll.77C78B40
00401119 call edx
0040111A mov eax, 88
0040111B mov edx, ntdll.77C78B40
0040111C call edx
0040111D mov eax, 89
0040111E mov edx, ntdll.77C78B40
0040111F call edx
00401120 mov eax, 8A
00401121 mov edx, ntdll.77C78B40
00401122 call edx
00401123 mov eax, 8B
00401124 mov edx, ntdll.77C78B40
00401125 call edx
00401126 mov eax, 8C
00401127 mov edx, ntdll.77C78B40
00401128 call edx
00401129 mov eax, 8D
0040112A mov edx, ntdll.77C78B40
0040112B call edx
0040112C mov eax, 8E
0040112D mov edx, ntdll.77C78B40
0040112E call edx
0040112F mov eax, 8F
00401130 mov edx, ntdll.77C78B40
00401131 call edx
00401132 mov eax, 90
00401133 mov edx, ntdll.77C78B40
00401134 call edx
00401135 mov eax, 91
00401136 mov edx, ntdll.77C78B40
00401137 call edx
00401138 mov eax, 92
00401139 mov edx, ntdll.77C78B40
0040113A call edx
0040113B mov eax, 93
0040113C mov edx, ntdll.77C78B40
0040113D call edx
0040113E mov eax, 94
0040113F mov edx, ntdll.77C78B40
00401140 call edx
00401141 mov eax, 95
00401142 mov edx, ntdll.77C78B40
00401143 call edx
00401144 mov eax, 96
00401145 mov edx, ntdll.77C78B40
00401146 call edx
00401147 mov eax, 97
00401148 mov edx, ntdll.77C78B40
00401149 call edx
0040114A mov eax, 98
0040114B mov edx, ntdll.77C78B40
0040114C call edx
0040114D mov eax, 99
0040114E mov edx, ntdll.77C78B40
0040114F call edx
00401150 mov eax, 9A
00401151 mov edx, ntdll.77C78B40
00401152 call edx
00401153 mov eax, 9B
00401154 mov edx, ntdll.77C78B40
00401155 call edx
00401156 mov eax, 9C
00401157 mov edx, ntdll.77C78B40
00401158 call edx
00401159 mov eax, 9D
0040115A mov edx, ntdll.77C78B40
0040115B call edx
0040115C mov eax, 9E
0040115D mov edx, ntdll.77C78B40
0040115E call edx
0040115F mov eax, 9F
00401160 mov edx, ntdll.77C78B40
00401161 call edx
00401162 mov eax, A0
00401163 mov edx, ntdll.77C78B40
00401164 call edx
00401165 mov eax, A1
00401166 mov edx, ntdll.77C78B40
00401167 call edx
00401168 mov eax, A2
00401169 mov edx, ntdll.77C78B40
0040116A call edx
0040116B mov eax, A3
0040116C mov edx, ntdll.77C78B40
0040116D call edx
0040116E mov eax, A4
0040116F mov edx, ntdll.77C78B40
00401170 call edx
0040116F mov eax, A5
00401171 mov edx, ntdll.77C78B40
00401172 call edx
00401170 mov eax, A6
00401172 mov edx, ntdll.77C78B40
00401173 call edx
00401171 mov eax, A7
00401173 mov edx, ntdll.77C78B40
00401174 call edx
00401172 mov eax, A8
00401174 mov edx, ntdll.77C78B40
00401175 call edx
00401173 mov eax, A9
00401175 mov edx, ntdll.77C78B40
00401176 call edx
00401174 mov eax, AA
00401176 mov edx, ntdll.77C78B40
00401177 call edx
00401175 mov eax, AB
00401177 mov edx, ntdll.77C78B40
00401178 call edx
00401176 mov eax, AC
00401178 mov edx, ntdll.77C78B40
00401179 call edx
00401177 mov eax, AD
00401179 mov edx, ntdll.77C78B40
0040117A call edx
00401178 mov eax, AE
0040117A mov edx, ntdll.77C78B40
0040117B call edx
00401179 mov eax, AF
0040117B mov edx, ntdll.77C78B40
0040117C call edx
0040117A mov eax, B0
0040117C mov edx, ntdll.77C78B40
0040117D call edx
0040117B mov eax, B1
0040117D mov edx, ntdll.77C78B40
0040117E call edx
0040117C mov eax, B2
0040117E mov edx, ntdll.77C78B40
0040117F call edx
0040117D mov eax, B3
0040117F mov edx, ntdll.77C78B40
00401180 call edx
0040117E mov eax, B4
00401180 mov edx, ntdll.77C78B40
00401181 call edx
0040117F mov eax, B5
00401181 mov edx, ntdll.77C78B40
00401182 call edx
00401180 mov eax, B6
00401182 mov edx, ntdll.77C78B40
00401183 call edx
00401181 mov eax, B7
00401183 mov edx, ntdll.77C78B40
00401184 call edx
00401182 mov eax, B8
00401184 mov edx, ntdll.77C78B40
00401185 call edx
00401183 mov eax, B9
00401185 mov edx, ntdll.77C78B40
00401186 call edx
00401184 mov eax, BA
00401186 mov edx, ntdll.77C78B40
00401187 call edx
00401185 mov eax, BB
00401187 mov edx, ntdll.77C78B40
00401188 call edx
00401186 mov eax, BC
00401188 mov edx, ntdll.77C78B40
00401189 call edx
00401187 mov eax, BD
00401189 mov edx, ntdll.77C78B40
0040118A call edx
00401188 mov eax, BE
0040118A mov edx, ntdll.77C78B40
0040118B call edx
00401189 mov eax, BF
0040118B mov edx, ntdll.77C78B40
0040118C call edx
0040118A mov eax, C0
0040118C mov edx, ntdll.77C78B40
0040118D call edx
0040118B mov eax, C1
0040118D mov edx, ntdll.77C78B40
0040118E call edx
0040118C mov eax, C2
0040118E mov edx, ntdll.77C78B40
0040118F call edx
0040118D mov eax, C3
0040118F mov edx, ntdll.77C78B40
00401190 call edx
0040118E mov eax, C4
00401190 mov edx, ntdll.77C78B40
00401191 call edx
0040118F mov eax, C5
00401191 mov edx, ntdll.77C78B40
00401192 call edx
0040118A mov eax, C6
00401192 mov edx, ntdll.77C78B40
00401193 call edx
0040118B mov eax, C7
00401193 mov edx, ntdll.77C78B40
00401194 call edx
0040118C mov eax, C8
00401194 mov edx, ntdll.77C78B40
00401195 call edx
0040118D mov eax, C9
00401195 mov edx, ntdll.77C78B40
00401196 call edx
0040118E mov eax, CA
00401196 mov edx, ntdll.77C78B40
00401197 call edx
0040118F mov eax, CB
00401197 mov edx, ntdll.77C78B40
00401198 call edx
00401190 mov eax, CC
00401198 mov edx, ntdll.77C78B40
00401199 call edx
00401191 mov eax, CD
00401199 mov edx, ntdll.77C78B40
0040119A call edx
00401192 mov eax, CE
0040119A mov edx, ntdll.77C78B40
0040119B call edx
00401193 mov eax, CF
0040119B mov edx, ntdll.77C78B40
0040119C call edx
00401194 mov eax, D0
0040119C mov edx, ntdll.77C78B40
0040119D call edx
00401195 mov eax, D1
0040119D mov edx, ntdll.77C78B40
0040119E call edx
00401196 mov eax, D2
0040119E mov edx, ntdll.77C78B40
0040119F call edx
00401197 mov eax, D3
0040119F mov edx, ntdll.77C78B40
004011A0 call edx
00401198 mov eax, D4
004011A0 mov edx, ntdll.77C78B40
004011A1 call edx
00401199 mov eax, D5
004011A1 mov edx, ntdll.77C78B40
004011A2 call edx
0040119A mov eax, D6
004011A2 mov edx, ntdll.77C78B40
004011A3 call edx
0040119B mov eax, D7
004011A3 mov edx, ntdll.77C78B40
004011A4 call edx
0040119C mov eax, D8
004011A4 mov edx, ntdll.77C78B40
004011A5 call edx
0040119D mov eax, D9
004011A5 mov edx, ntdll.77C78B40
004011A6 call edx
0040119E mov eax, DA
004011A6 mov edx, ntdll.77C78B40
004011A7 call edx
0040119F mov eax, DB
004011A7 mov edx, ntdll.77C78B40
004011A8 call edx
004011A0 mov eax, DC
004011A8 mov edx, ntdll.77C78B40
004011A9 call edx
004011A1 mov eax, DD
004011A9 mov edx, ntdll.77C78B40
004011AA call edx
004011A2 mov eax, DE
004011AA mov edx, ntdll.77C78B40
004011AB call edx
004011A3 mov eax, DF
004011AB mov edx, ntdll.77C78B40
004011AC call edx
004011A4 mov eax, E0
004011AC mov edx, ntdll.77C78B40
004011AD call edx
004011A5 mov eax, E1
004011AD mov edx, ntdll.77C78B40
004011AE call edx
004011A6 mov eax, E2
004011AE mov edx, ntdll.77C78B40
004011AF call edx
004011A7 mov eax, E3
004011AF mov edx, ntdll.77C78B40
004011B0 call edx
004011A8 mov eax, E4
004011B0 mov edx, ntdll.77C78B40
004011B1 call edx
004011A9 mov eax, E5
004011B1 mov edx, ntdll.77C78B40
004011B2 call edx
004011AA mov eax, E6
004011B2 mov edx, ntdll.77C78B40
004011B3 call edx
004011AB mov eax, E7
004011B3 mov edx, ntdll.77C78B40
004011B4 call edx
004011AC mov eax, E8
004011B4 mov edx, ntdll.77C78B40
004011B5 call edx
004011AD mov eax, E9
004011B5 mov edx, ntdll.77C78B40
004011B6 call edx
004011AE mov eax, EA
004011B6 mov edx, ntdll.77C78B40
004011B7 call edx
004011AF mov eax, EB
004011B7 mov edx, ntdll.77C78B40
004011B8 call edx
004011B0 mov eax, EC
004011B8 mov edx, ntdll.77C78B40
004011B9 call edx
004011B1 mov eax, ED
004011B9 mov edx, ntdll.77C78B40
004011BA call edx
004011B2 mov eax, EE
004011BA mov edx, ntdll.77C78B40
004011BB call edx
004011B3 mov eax, EF
004011BB mov edx, ntdll.77C78B40
004011BC call edx
004011B4 mov eax, F0
004011BC mov edx, ntdll.77C78B40
004011BD call edx
004011B5 mov eax, F1
004011BD mov edx, ntdll.77C78B40
004011BE call edx
004011B6 mov eax, F2
004011BE mov edx, ntdll.77C78B40
004011BF call edx
004011B7 mov eax, F3
004011BF mov edx, ntdll.77C78B40
004011C0 call edx
004011B8 mov eax, F4
004011C0 mov edx, ntdll.77C78B40
004011C1 call edx
004011B9 mov eax, F5
004011C1 mov edx, ntdll.77C78B40
004011C2 call edx
004011BA mov eax, F6
004011C2 mov edx, ntdll.77C78B40
004011C3 call edx
004011BB mov eax, F7
004011C3 mov edx, ntdll.77C78B40
004011C4 call edx
004011BC mov eax, F8
004011C4 mov edx, ntdll.77C78B40
004011C5 call edx
004011BD mov eax, F9
004011C5 mov edx, ntdll.77C78B40
004011C6 call edx
004011BE mov eax, FA
004011C6 mov edx, ntdll.77C78B40
004011C7 call edx
004011BF mov eax, FB
004011C7 mov edx, ntdll.77C78B40
004011C8 call edx
004011C0 mov eax, FC
004011C8 mov edx, ntdll.77C78B40
004011C9 call edx
004011C1 mov eax, FD
004011C9 mov edx, ntdll.77C78B40
004011CA call edx
004011C2 mov eax, FE
004011CA mov edx, ntdll.77C78B40
004011CB call edx
004011C3 mov eax, FF
004011CB mov edx, ntdll.77C78B40
004011CC call edx
```

Memory Dump:

```
Address Hex
00600060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00600070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00600080 55 48 89 E8 48 83 EC 40 53 56 57 41 54 48 83 EC
00600090 30 E8 27 00 00 00 06 01 01 00 00 00 00 00 00 00
006000A0 28 07 00 00 00 00 64 19 95 00 00 00 00 55 78
006000B0 53 75 62 63 49 6E 66 6F 0C 8B 6A 60 00 00 00 00
006000C0 58 65 48 88 00 48 88 40 18 48 80 78 30 6A 02 5E
006000D0 48 89 7D C0 66 85 F6 53 48 88 3F 48 58 7D C0
006000E0 74 4A 0F 86 4A 88 C9 7A 68 05 15 00 00 54
006000F0 89 D0 C1 E2 05 01 C2 48 88 47 40 0F B6 44 08 FF
00600100 24 DF 01 C2 E2 8A FA 98 E8 2A 83 75 08 FF 77
00600110 10 8F 45 C8 48 FF CE E8 8B 81 FA 13 2D 49 28 75
00600120 09 FF 77 10 88 48 FF CE E8 8B 81 FA 13 2D 49 28 75
00600130 45 88 48 3C 4F 8D 0C 01 68 00 00 00 45 88 11 4D
00600140 85 D2 74 58 4F 8D 10 41 88 48 18 45 88 63 2D
00600150 49 8D 3C 4F 8D 0C 01 68 00 00 00 45 88 11 4D
00600160 15 00 00 5A 89 D0 C1 E2 05 01 C2 31 C0 AC 01 C2
00600170 85 C0 75 F0 81 FA 13 2D 49 28 75 08 FF 77
00600180 00 00 00 41 88 7B 24 4C 01 C7 66 88 0C 4F 41 8B
00600190 7B 1C 4C 01 C7 66 88 0C 4F 41 8B 89 45 D8 E8
006001A0 02 00 00 45 88 7B 24 4C 01 C7 66 88 0C 4F 41 8B
006001B0 00 58 48 88 4D C8 48 89 C2 FF 55 D8 48 89 45 E8
006001C0 E8 0C 00 00 63 6C 6F 75 48 81 6E 64 6C 65
006001D0 00 58 48 88 4D C8 48 89 C2 FF 55 D8 48 89 45 E8
006001E0 E8 09 00 00 53 65 74 50 72 6F 70 41 00 58 48
006001F0 88 4D 00 48 89 C2 FF 55 D8 48 89 45 E8 48 83 7B
00600200 10 00 74 23 48 31 C0 48 89 C1 48 89 C2 4C 8B 43
00600210 10 49 89 C1 48 89 44 24 20 48 89 44 24 28 FF 55
00600220 E8 48 89 C1 FF 55 F0 48 8D 43 18 48 88 08 48 89
00600230 C2 4C 8B 43 08 FF 55 E0 48 83 C4 30 41 5C 5F 5E
00600240 58 C9 00 00 00 00 00 00 00 00 00 00 00 00 00
00600250 00 00 
```

UxSubClass Redirection

- SetPropA()
- Redirects explorer.exe's properties to point to the malicious UxSubClassInfo



SetPropA function (winuser.h)

Article • 02/10/2023 • 2 minutes to read

[Feedback](#)

In this article

- Syntax
- Parameters
- Return value
- Remarks
- Requirements
- See also

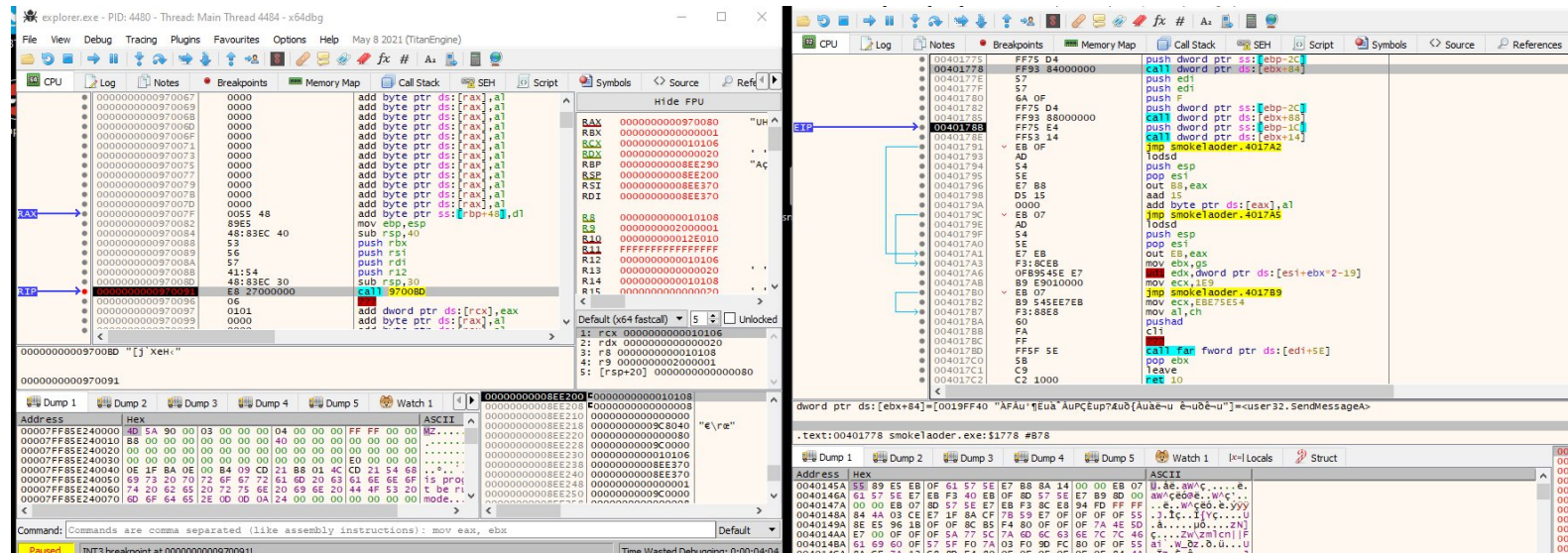
Adds a new entry or changes an existing entry in the property list of the specified window. The function adds a new entry to the list if the specified character string does not exist already in the list. The new entry contains the string and the handle. Otherwise, the function replaces the string's current handle with the specified handle.

Syntax

```
C++  
BOOL SetPropA(  
    [in] HWND hWnd,  
    [in] LPCSTR lpString,  
    [in, optional] HANDLE hData  
);
```


ShellCode Execution

- By Executing SendMessageA & SendNotifyMessageA
 - Explorer.exe with the modified property should now:
 - Execute the malicious UxSubClassInfo Structure
 - Which points to the injected shellcode
 - Which usually means the second stage malware is downloaded and installed
 - Ie... Cobalt Strike, Raccoon Stealer, Redline, IcedID



DEMO TIME!



References & Thanks

- [NightWolfs Smokeloader analysis](#)
- [Mario Ciccarelli's guide](#)
- [Pete Cowman's blog](#)
- [Cape Sandbox](#)
- [Herrcore](#) from [OALabs](#) for reading over my presentation
- [Pim's talk on Smokeloader](#)
- [Geoff Chappells](#) Documentation of [PEB](#) and [TEB](#)
- [Hexacorn's Propagate Injection Discovery](#)