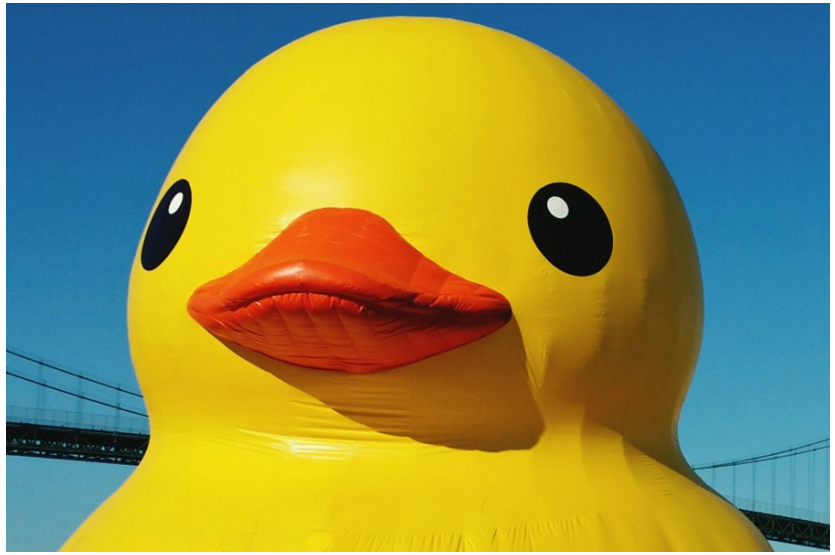
SmokeLoader Analysis

Kent Pang

VARSITY College

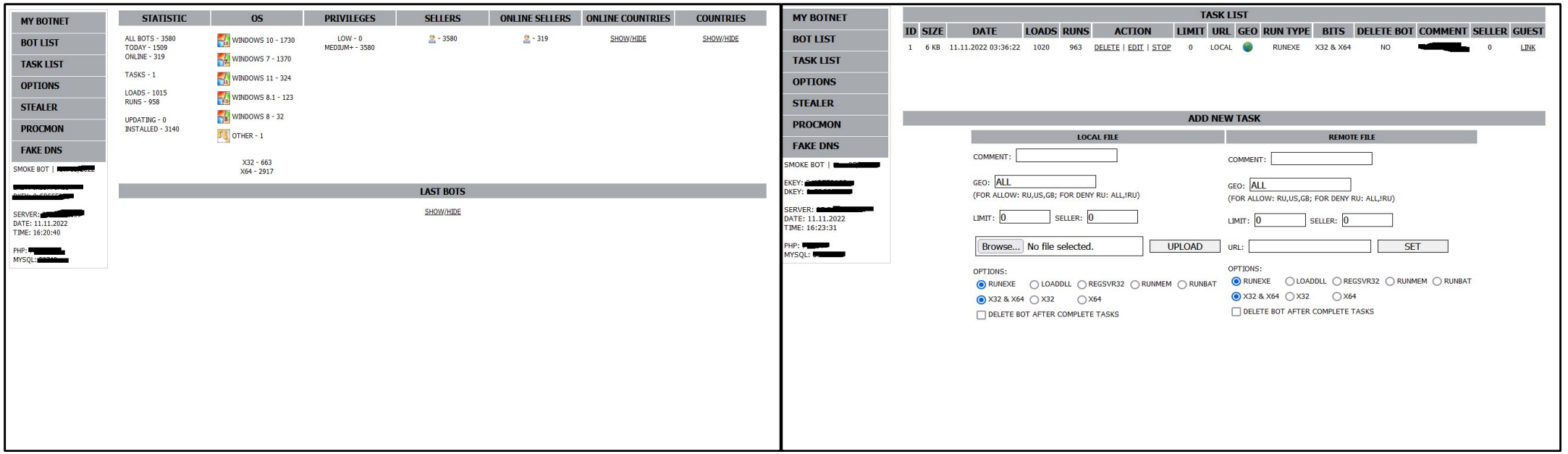
Iamwho <

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



SmokeLoader

- A loader type malware
- Highly obfuscated
- Extremely common



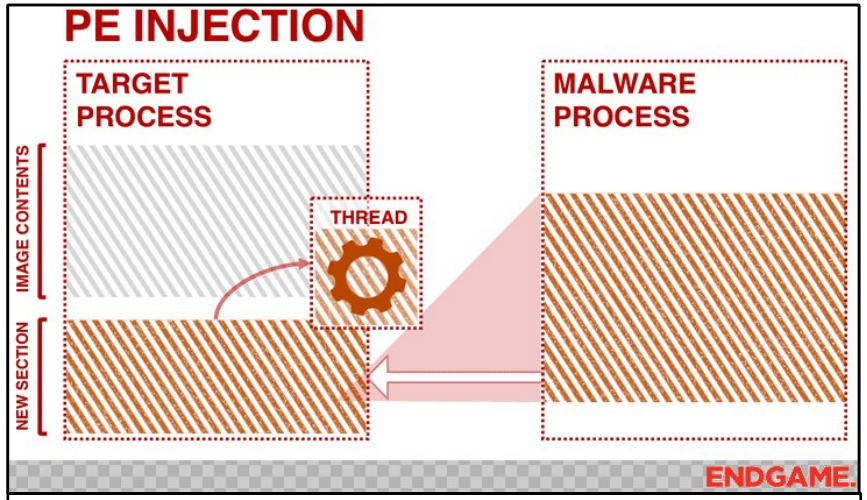
Source: [VxUnderground's](#) twitter

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

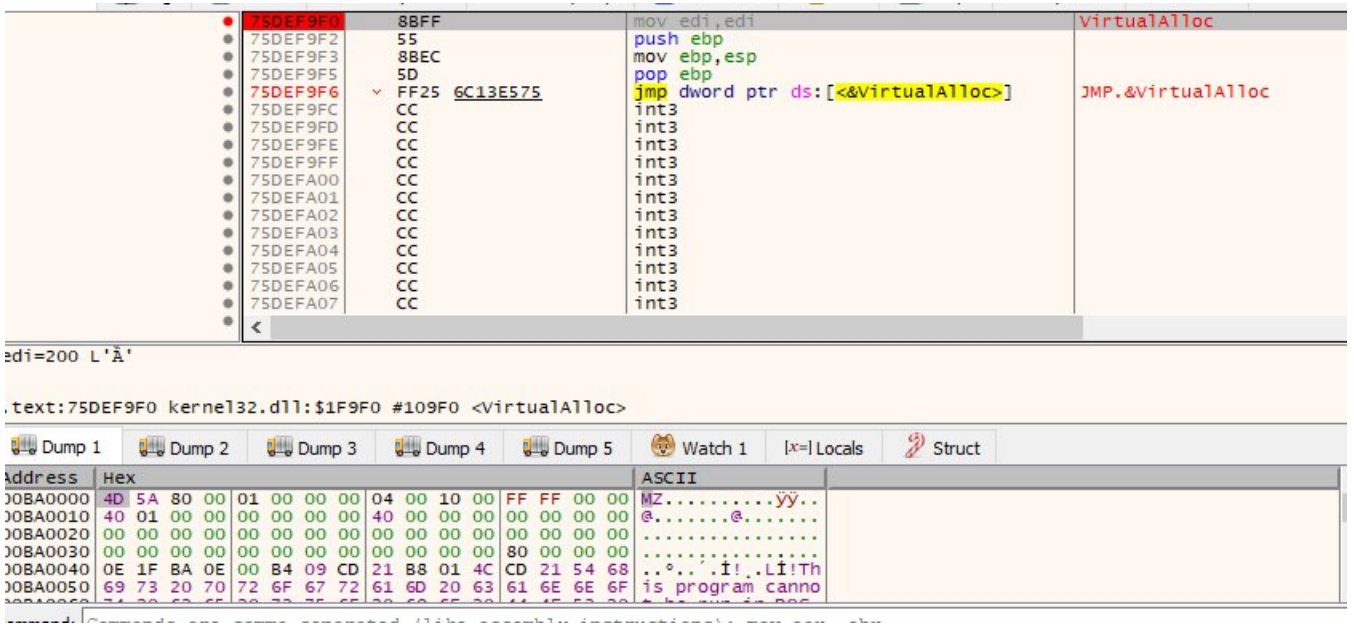


Source – [Ashkan Hosseini]

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)



VARSITY College

Stage 2

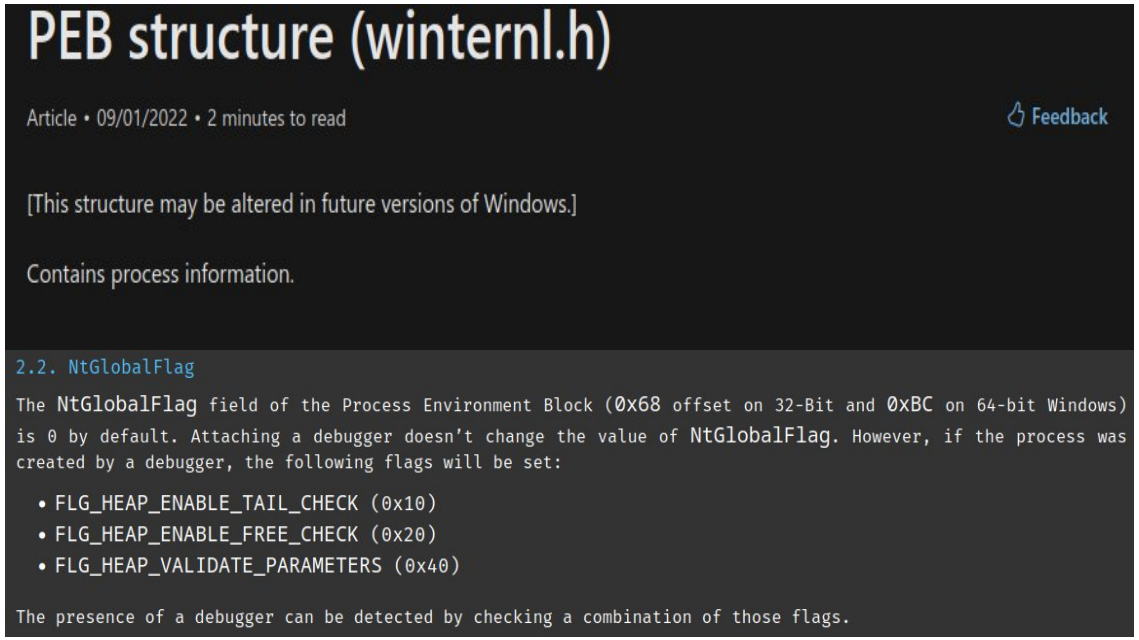
Pain.jpeg

Obfuscation Techniques

Aka funny text make life hard

Anti-Analysis

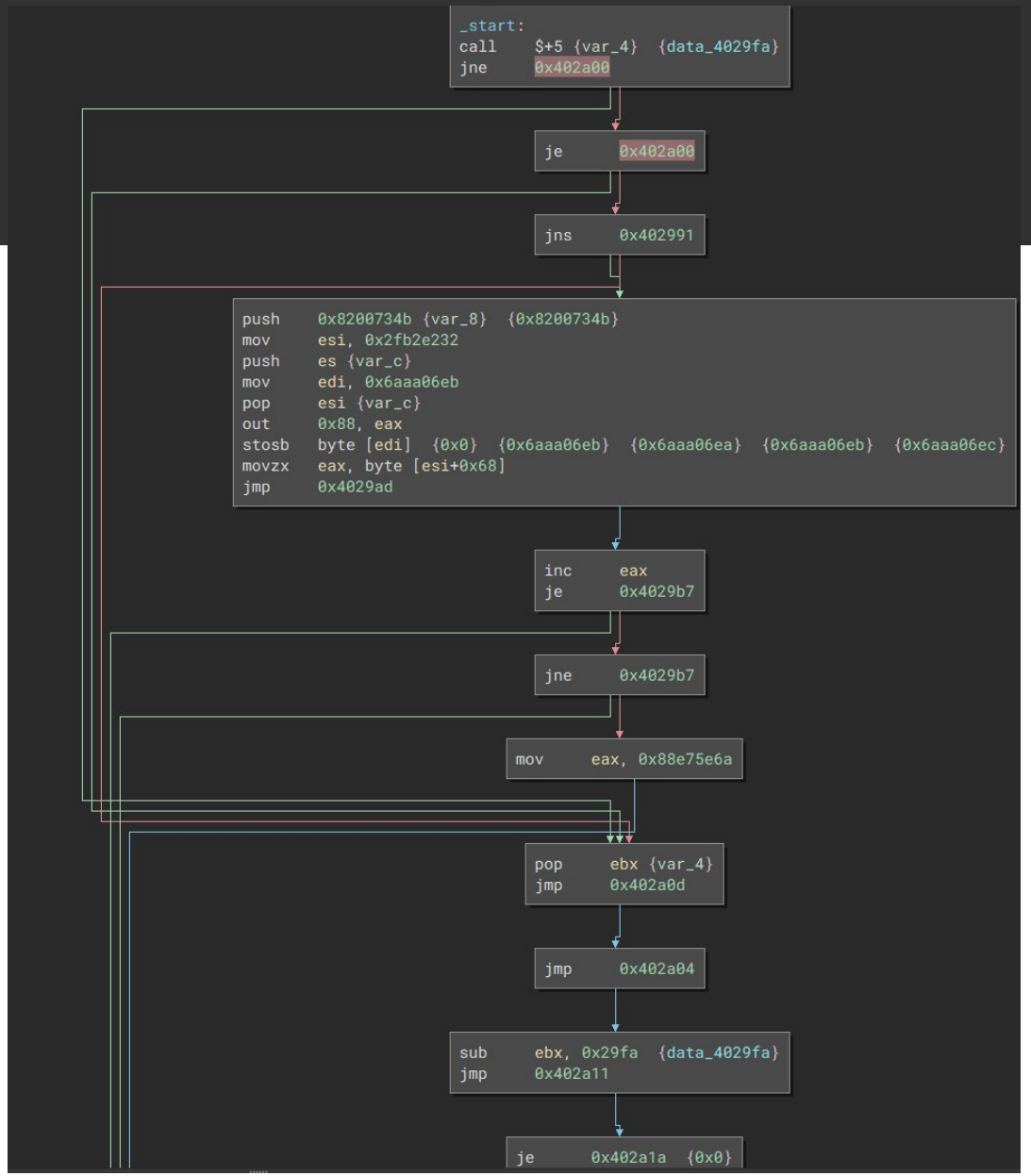
- TEB & PEB
  - Thread Environment Block & Process Environment Block
    - What Is TEB & PEB?
      - ISDebugged? 0x30 -> 0x02
      - NTGlobal Flag? 0x30 -> 0x68
- Avoids the need to call APIs



[CheckPoint's AntiDebug List]

Opaque Predicates

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



VARSITY College

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

VM Detection

- Checks HKLM\CurrentControlSet\Enum\IDE & SCSI
  - Checks for anything that includes
    - QEMU
    - VBOX
    - VIRTIO
    - VMWARE
    - XEN

NtOpenKey	KeyHandle: 0x000000f8 DesiredAccess: KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\MACHINE\System\CurrentControlSet\Enum\IDE ObjectAttributes: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\IDE	success
NtQueryKey	KeyHandle: 0x000000f8 KeyInformation: KeyInformationClass: 2	failed
NtQueryKey	KeyHandle: 0x000000f8 KeyInformation: R\xffa7>\xffe1;\xffbb\xffd4\x01\x00\x00\x00\x00\xffff\xffff\xffff\xffff\x00\x00\x00\x00 \x04\x00\x00\x00j\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 KeyInformationClass: 2	success
NtOpenKey	KeyHandle: 0x000000f8 DesiredAccess: KEY_QUERY_VALUE|KEY_ENUMERATE_SUB_KEYS ObjectAttributesHandle: 0x00000000 ObjectAttributesName: \REGISTRY\MACHINE\System\CurrentControlSet\Enum\SCSI ObjectAttributes: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Enum\SCSI	success
NtQueryKey	KeyHandle: 0x000000f8 KeyInformation: KeyInformationClass: 2	failed
NtQueryKey	KeyHandle: 0x000000f8 KeyInformation: \xff9b\xffe7\xffa9E<\x04\xffca\x01\x00\x00\x00\x00\xffff\xffff\xffff\xffff\x00\x00\x00\x00 \x01\x00\x00\x00>\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00 KeyInformationClass: 2	success

Propagate Injection

Malicious code go brrrr

Propagate Injection

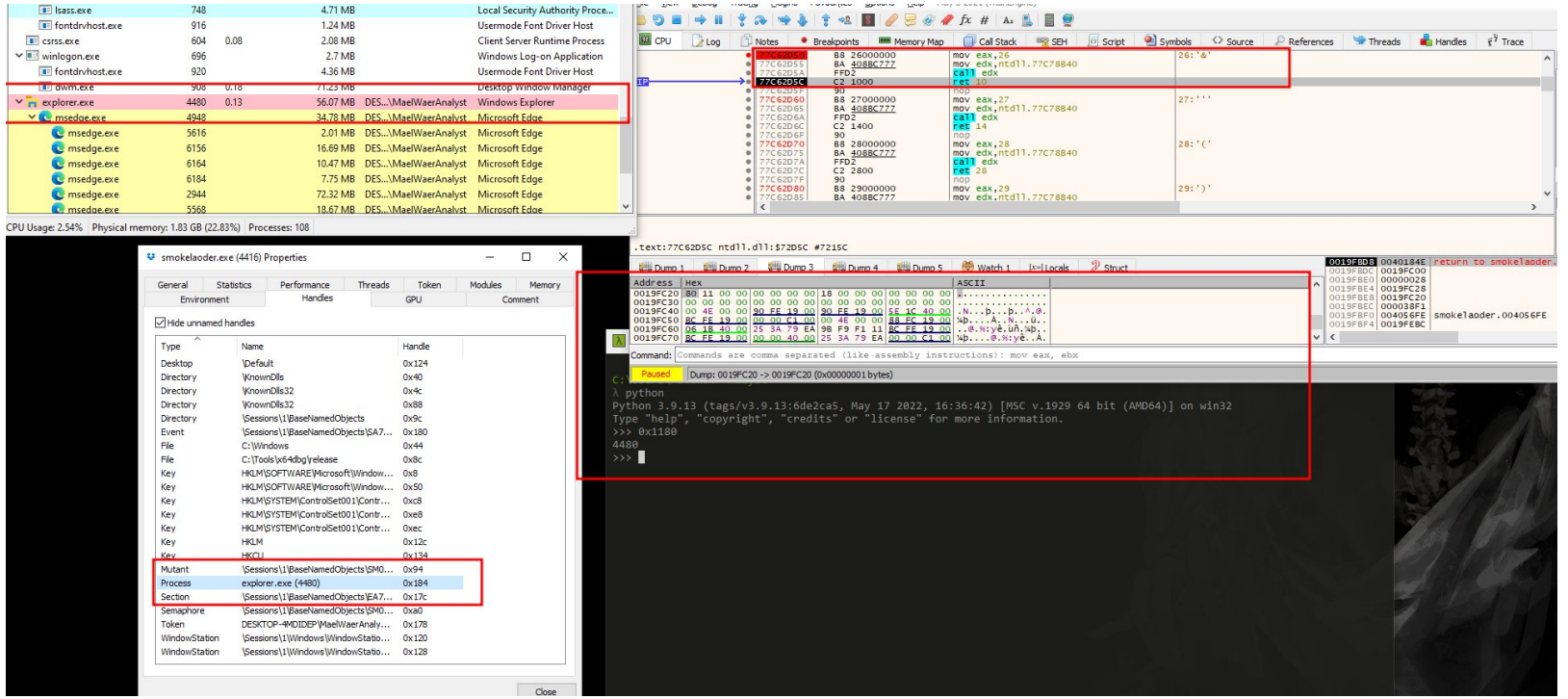
- Stealthy
- Doesn’t spawn external processes
- Performed by exploiting Window’s UxSubClassesInfo property
- Can really only be used to inject and execute shellcode

SmokeLoader Propagate Injection APIs

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

NtOpenProcess()

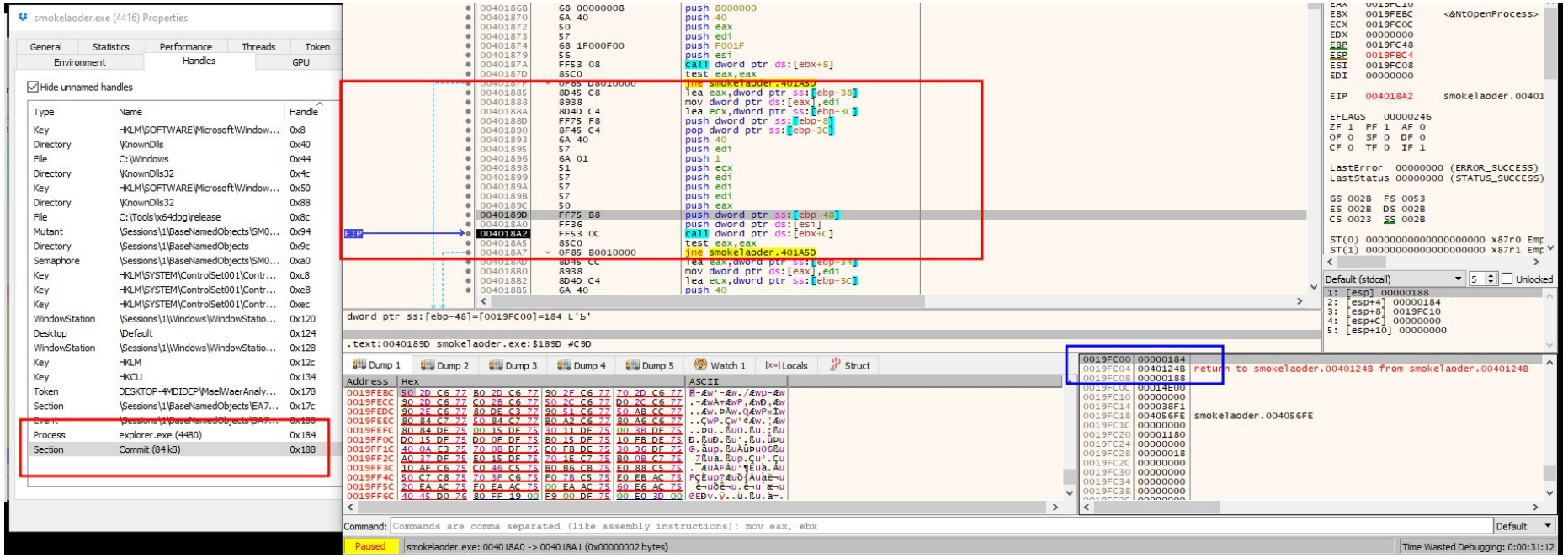
- The parent process creates an handle explorer.exe
- Allows the parent process to retrieve and manipulate the handled process



VARSITY College

Mapping Memory Space

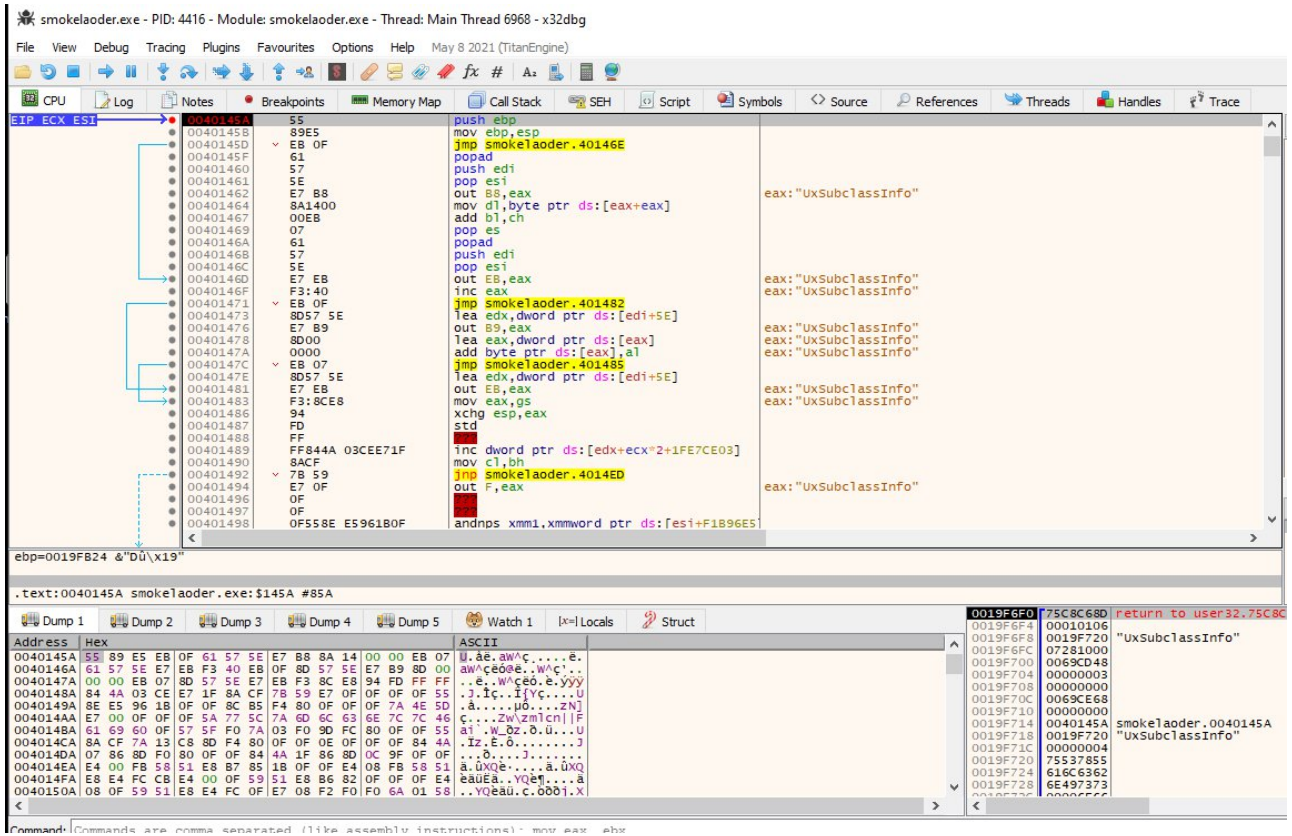
- Uses ZWCreateSection and ZwMapSection to allocate memory space into explorer.exe



VARSITY College

Locating UxSubClassInfo

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



VARSITY College

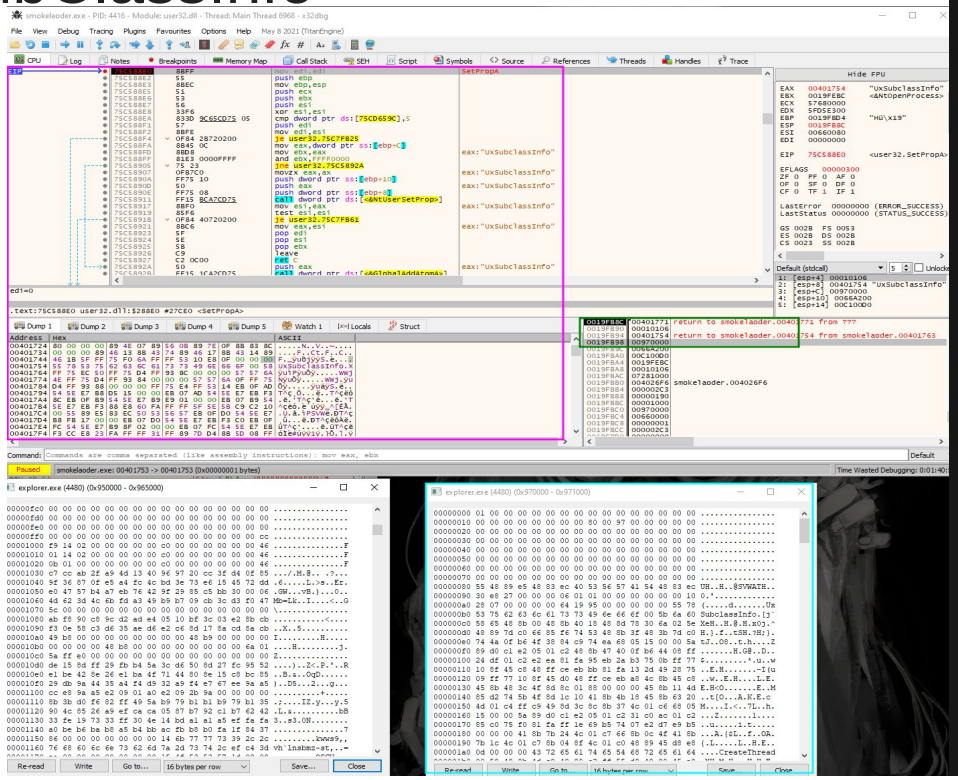
Struct Injection

- Injects the malicious UxSubClassInfo structure

- Follows the previous injection technique with ZwCreateSection & ZwMapSection

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

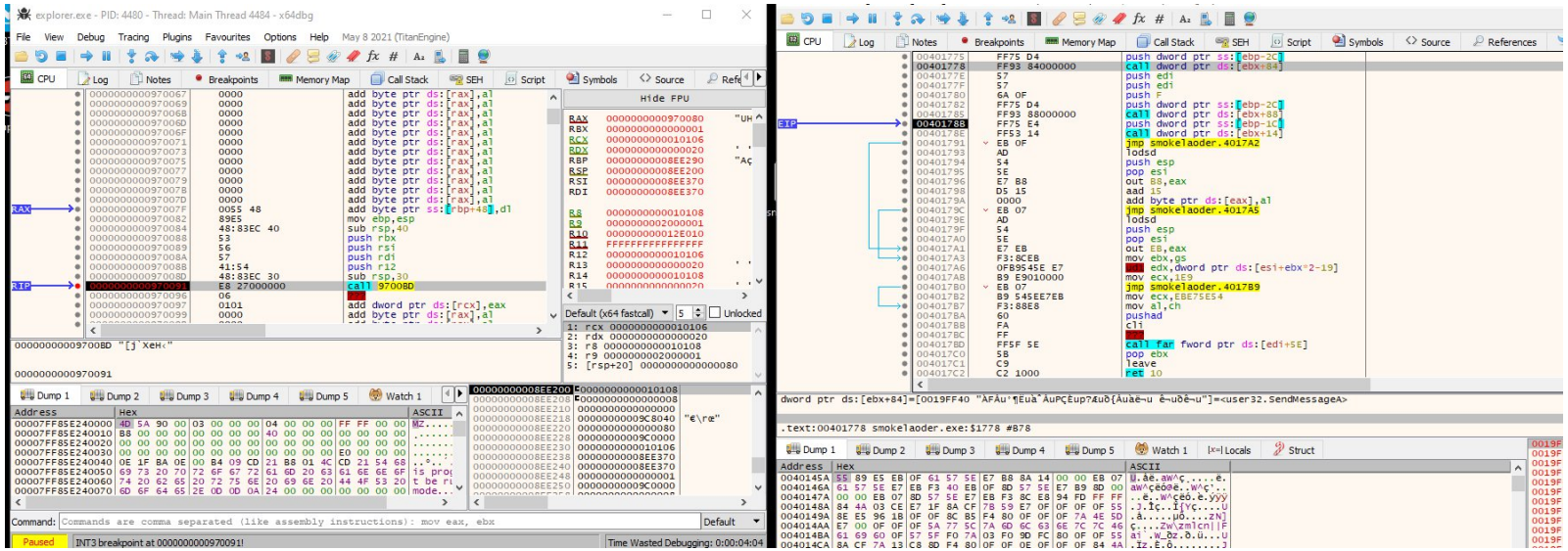
C++ Copy

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


VARSITY College

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