MalDev Essentials: Process Injection

[AFK.conf]

C# edition

PS > ls env:

- Offensive Security Accenture
- Twitter / GitHub @g0ttfrid
- Linkedin in/yurimaia

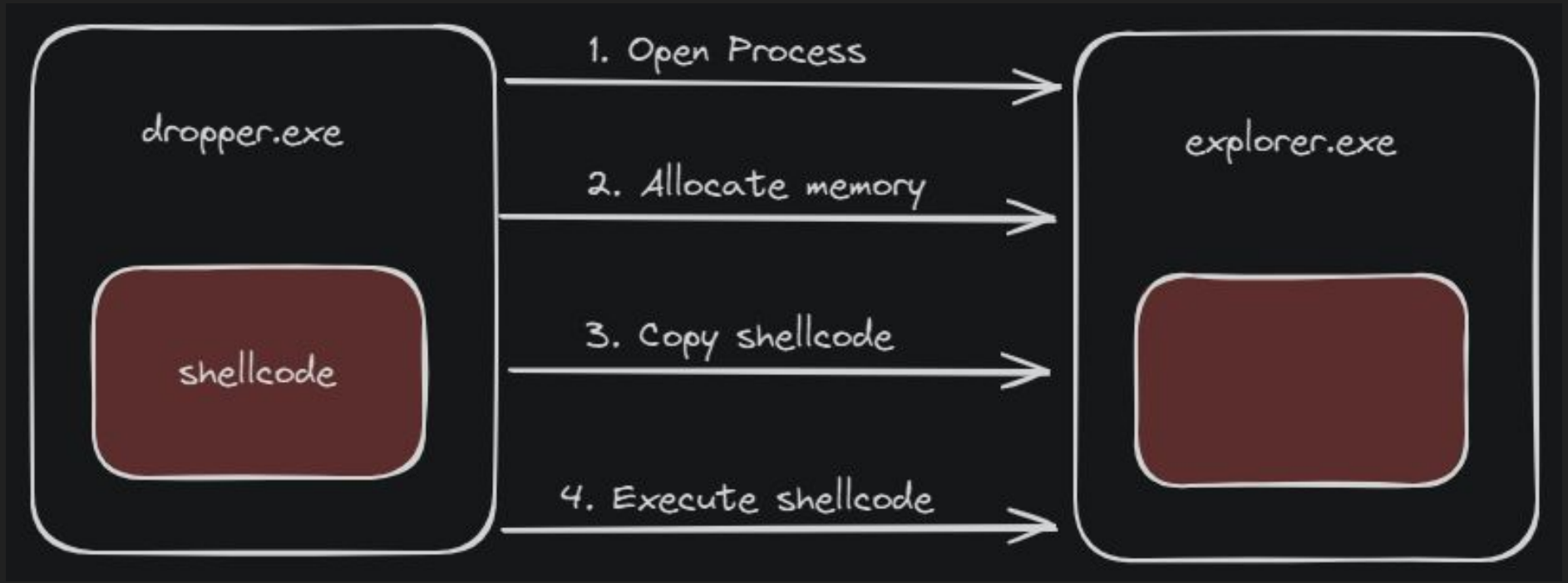
PS > Agenda

- Recap **Windows Internals 101**
- Process Injection
- WinAPI
- P/Invoke
- Process Hollowing
- Blue Team considerations

PS > Process Injection

- Escape from short-live process
- Change work context (eg. word.exe)
- C2 channel (TOON rule)

PS > Process Injection 101



PS > WinAPI | MSDN

1. OpenProcess
2. VirtualAllocEx
3. WriteProcessMemory
4. CreateRemoteThread

OpenProcess function (processthreadsapi.h)

Article • 10/31/2022 Feedback

In this article

Opens an existing local process object.

Syntax

C++ Copy

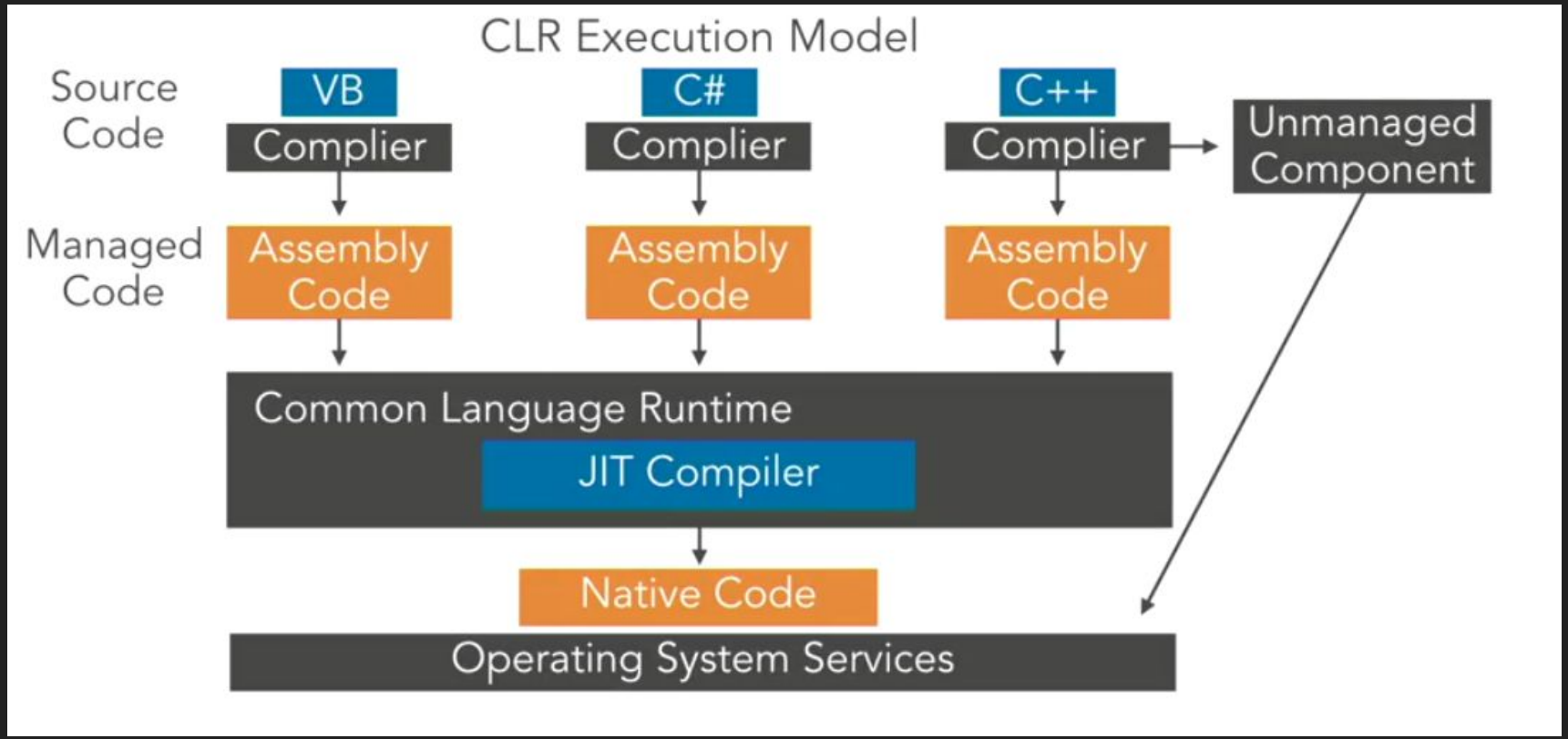
```
HANDLE OpenProcess(
  [in] DWORD dwDesiredAccess,
  [in] BOOL  bInheritHandle,
  [in] DWORD dwProcessId
);
```

Parameters

`[in] dwDesiredAccess`

The access to the process object. This access right is checked against the security descriptor for

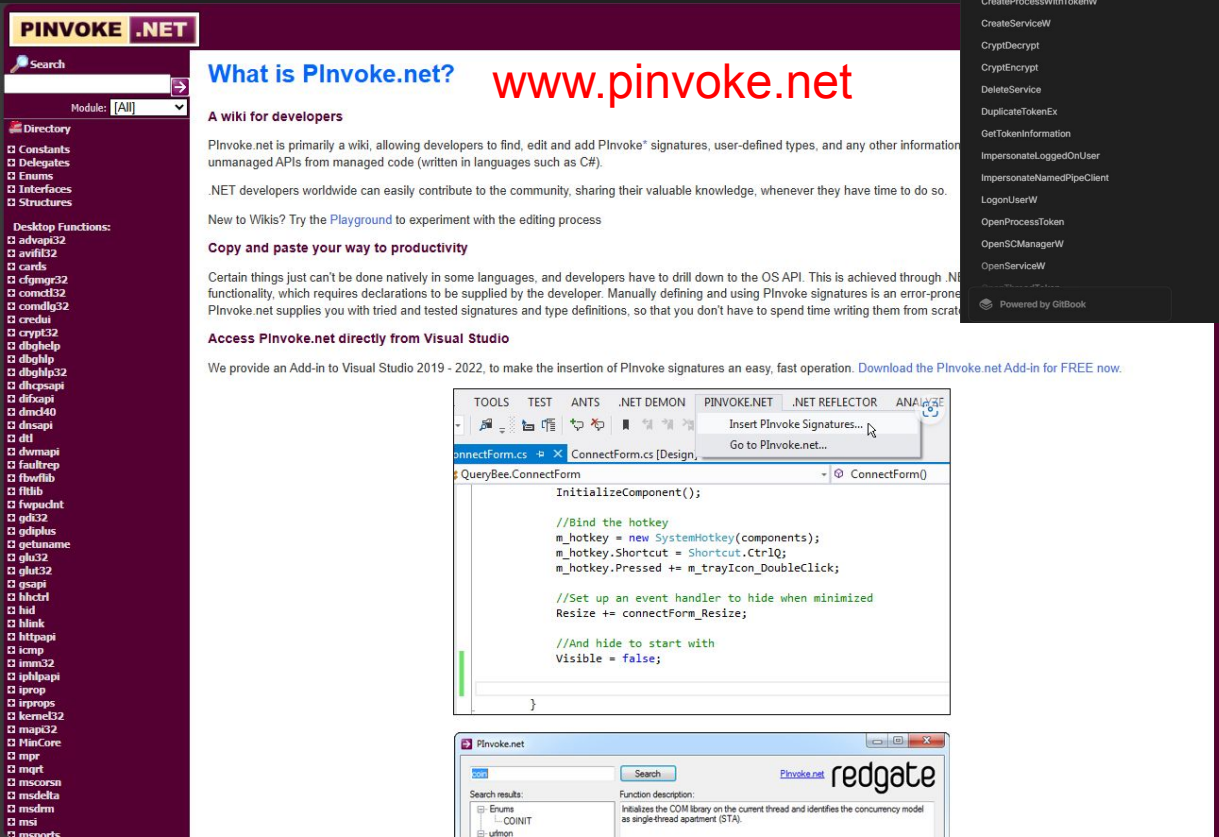
PS > WinAPI | Managed and Unmanaged Code

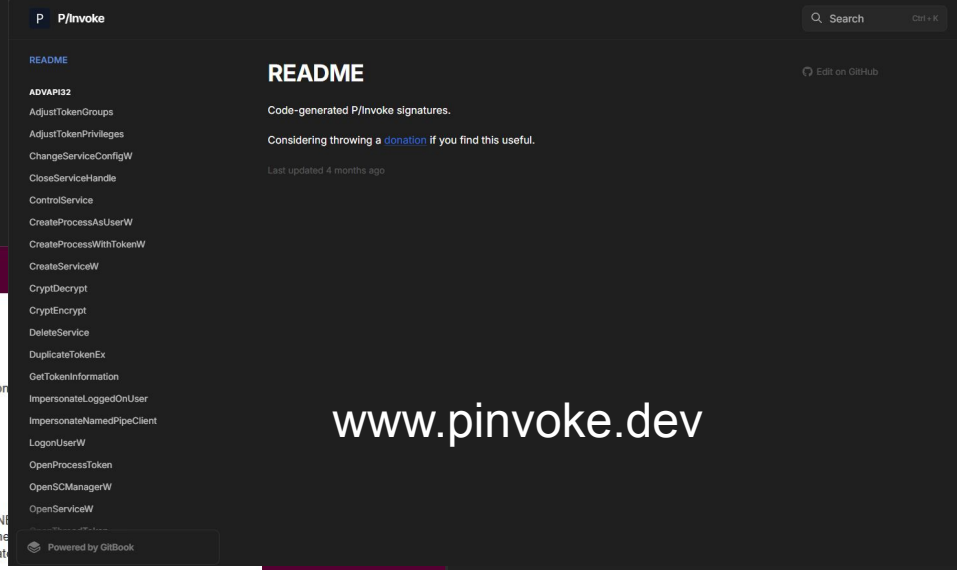


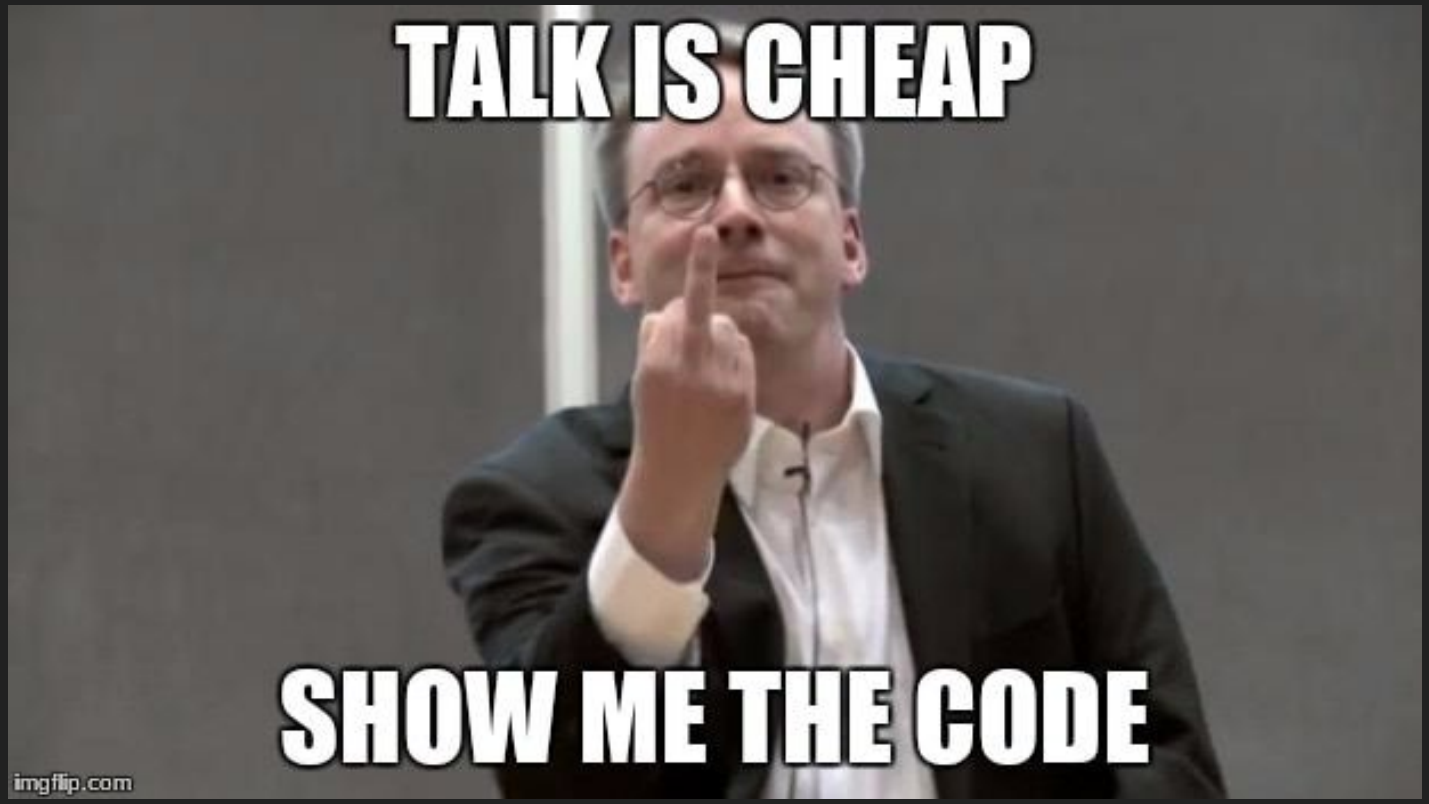
PS > P/Invoke

www.pinvoke.net

www.pinvoke.dev



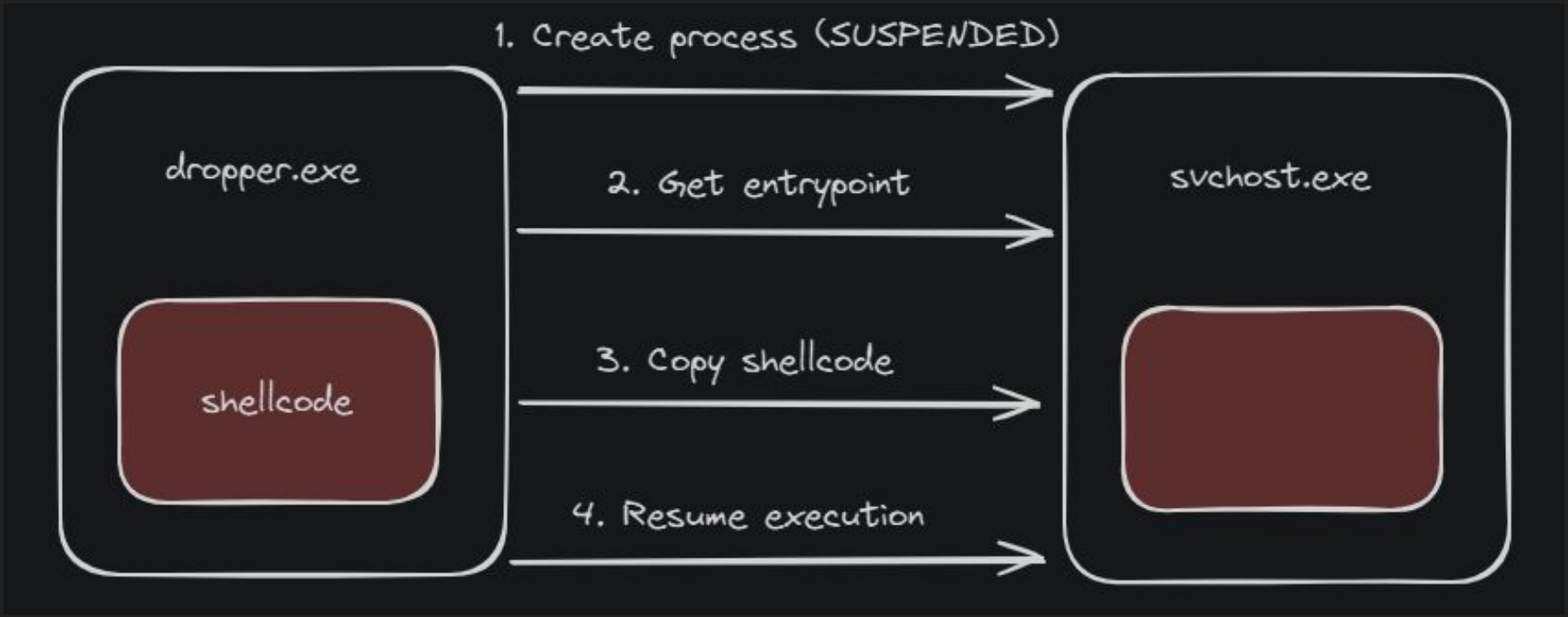


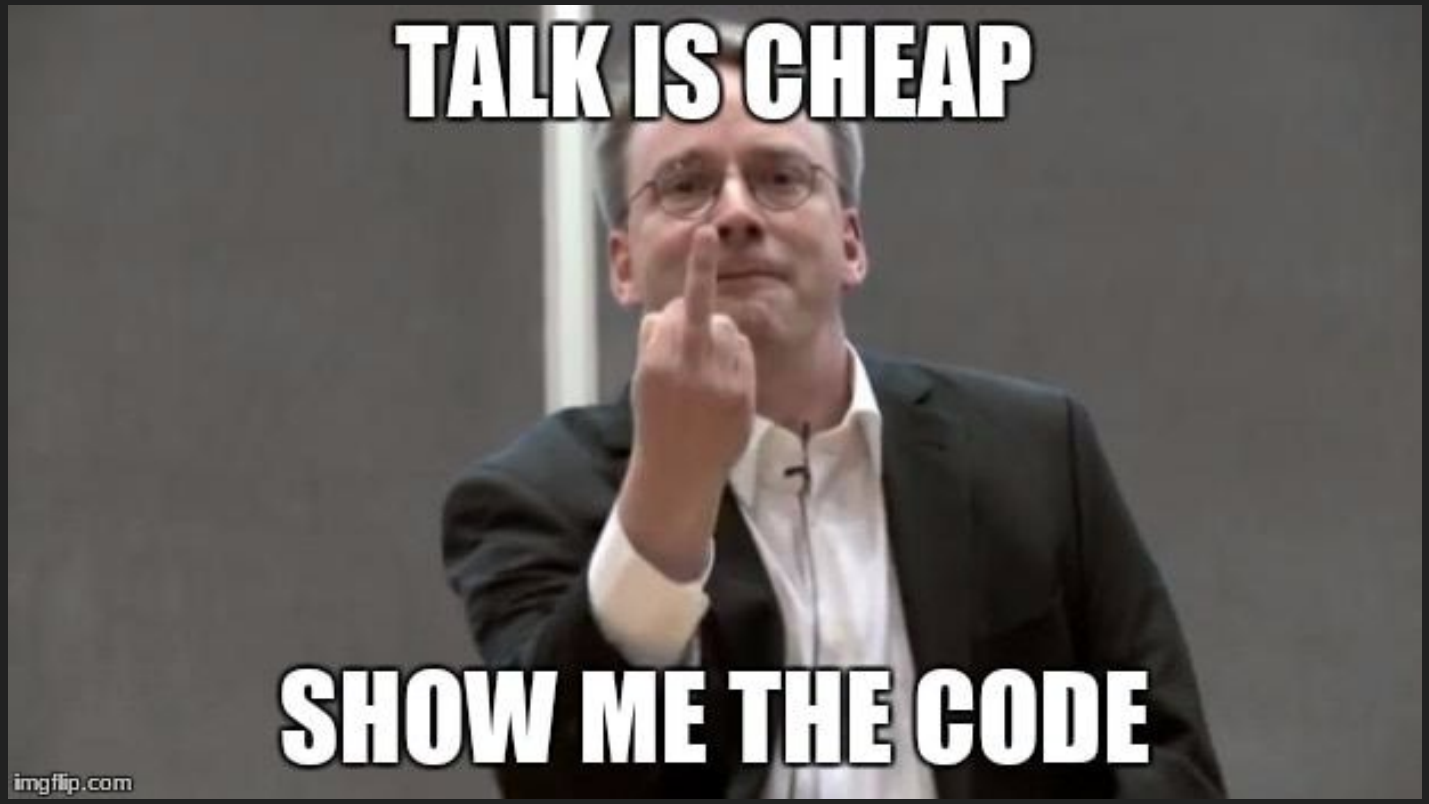

TALK IS CHEAP
SHOW ME THE CODE
imgflip.com

PS > Process Hollowing

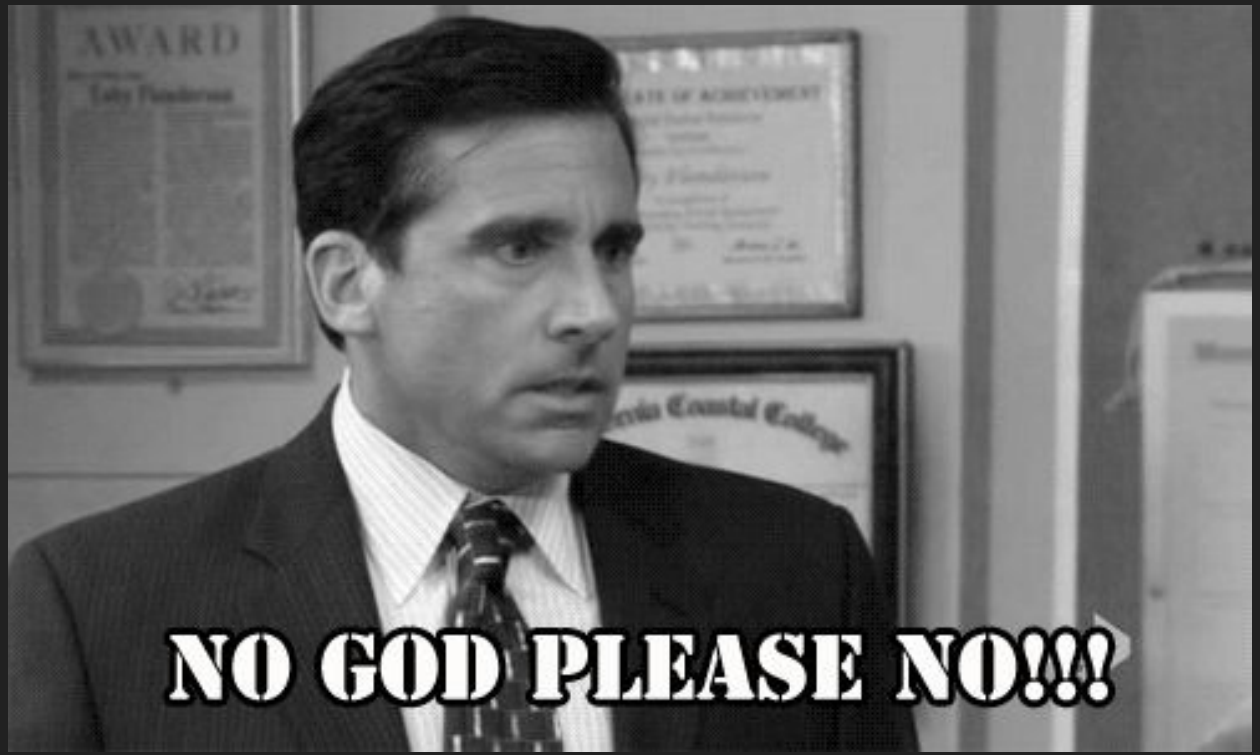
- Migration problem
- Create Process API
  - Creates the virtual memory space for the new process
  - Allocates the stack along with the Thread Environment Block (TEB)264 and the Process Environment Block (PEB)
  - Loads the required DLLs and the EXE into memory

PS > Process Hollowing




TALK IS CHEAP
SHOW ME THE CODE
imgflip.com

PS > Blue Team considerations



PS > refs

https://learn.microsoft.com/en-us/windows/win32/api/
https://learn.microsoft.com/en-us/dotnet/standard/native-interop/pinvoke
https://medium.com/@matterpreter/offensive-p-invoke-leveraging-the-win32-api-from-managed-code-7eef4fdef16d
https://crypt0ace.github.io/posts/Shellcode-Injection-Techniques-Part-2/
https://www.ired.team/offensive-security/code-injection-process-injection
https://redcanary.com/threat-detection-report/techniques/process-injection/

$$$
https://institute.sektor7.net/view/courses/red-team-operator-malware-development-essentials
https://training.zeropointsecurity.co.uk/courses/red-team-ops-ii
https://www.offsec.com/courses/pen-300/