

# MalDev Essentials: Process Injection

[ AFK.conf ]

C# edition

PS > ls env:

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



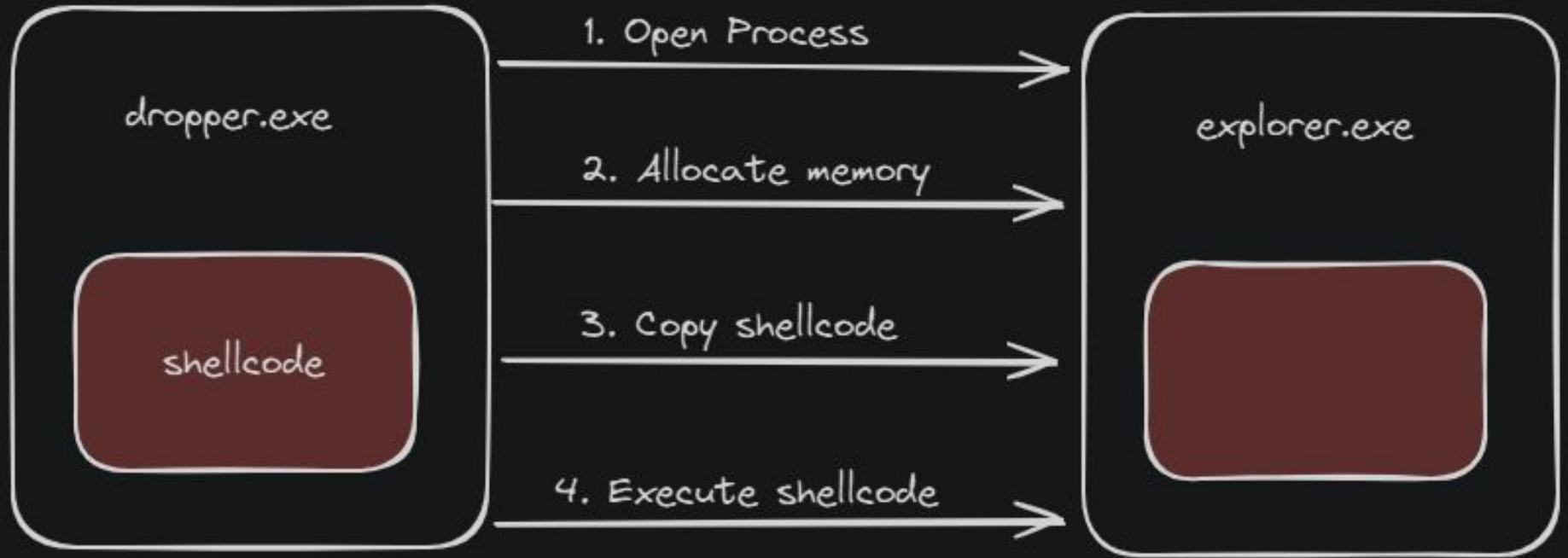
# PS > Agenda

- **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

[Syntax](#)

[Parameters](#)

[Return value](#)

[Remarks](#)

[Show 2 more](#)

Opens an existing local process object.

### Syntax

C++

[Copy](#)

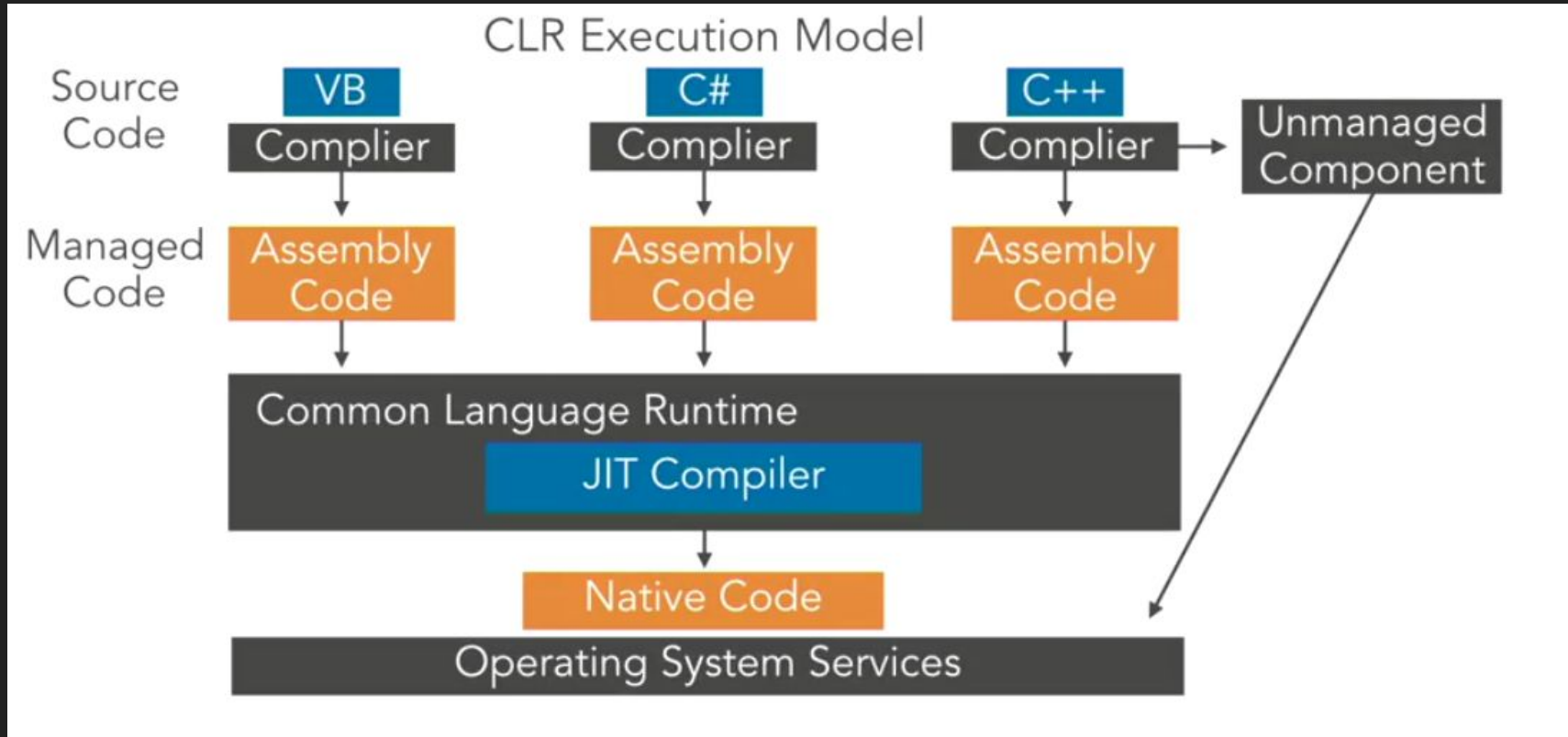
```
HANDLE OpenProcess(  
    [in] DWORD dwDesiredAccess,  
    [in] BOOL bInheritHandle,  
    [in] DWORD dwProcessId  
);
```

### 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

## PINVOKE .NET

Search

Module: [All]

Directory

Constants  
Delegates  
Enums  
Interfaces  
Structures

Desktop Functions:

advapi32  
avifil32  
cards  
cfgmgr32  
comctl32  
comdlg32  
credui  
crypt32  
dbghelp  
dbghlp  
dbghlp32  
dhcpcapi  
dibapi  
dmc40  
dmsapi  
dtd  
dwmapi  
faultrep  
fbwlib  
fltlb  
foxpudnt  
gd32  
gdiplus  
getuname  
glu32  
glut32  
gssapi  
hhctrl  
hid  
hlink  
hitapi  
icmp  
imm32  
ipbapi  
iprop  
irprops  
kernel32  
map32  
MinCore  
mpr  
mqrt  
mscorsn  
msdelta  
msdm  
msi  
msports

## What is PInvoke.net?

www.pinvoke.net

### A wiki for developers

PInvoke.net is primarily a wiki, allowing developers to find, edit and add PInvoke\* signatures, user-defined types, and any other information unmanaged APIs from managed code (written in languages such as C#).

.NET developers worldwide can easily contribute to the community, sharing their valuable knowledge, whenever they have time to do so.

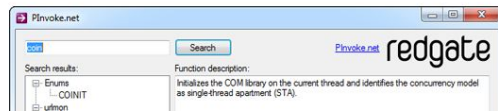
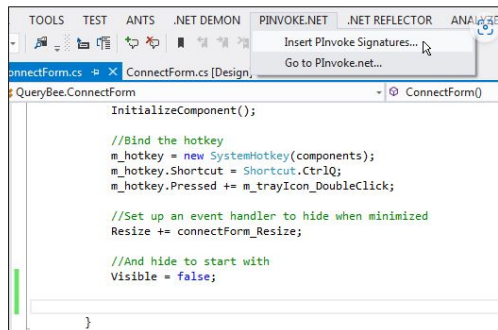
New to Wikis? Try the [Playground](#) to experiment with the editing process

### Copy and paste your way to productivity

Certain things just can't be done natively in some languages, and developers have to drill down to the OS API. This is achieved through .NET functionality, which requires declarations to be supplied by the developer. Manually defining and using PInvoke signatures is an error-prone. PInvoke.net supplies you with tried and tested signatures and type definitions, so that you don't have to spend time writing them from scratch.

### Access PInvoke.net directly from Visual Studio

We provide an Add-in to Visual Studio 2019 - 2022, to make the insertion of PInvoke signatures an easy, fast operation. [Download the PInvoke.net Add-in for FREE now.](#)



P/Invoke

README

ADVAPI32

AdjustTokenGroups

AdjustTokenPrivileges

ChangeServiceConfigW

CloseServiceHandle

ControlService

CreateProcessAsUserW

CreateProcessWithTokenW

CreateServiceW

CryptDecrypt

CryptEncrypt

DeleteService

DuplicateTokenEx

GetTokenInformation

ImpersonateLoggedOnUser

ImpersonateNamedPipeClient

LoginUserW

OpenProcessToken

OpenSCManagerW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

OpenServiceW

## README

Code-generated P/Invoke signatures.

Considering throwing a [donation](#) if you find this useful.

Last updated 4 months ago

www.pinvoke.dev



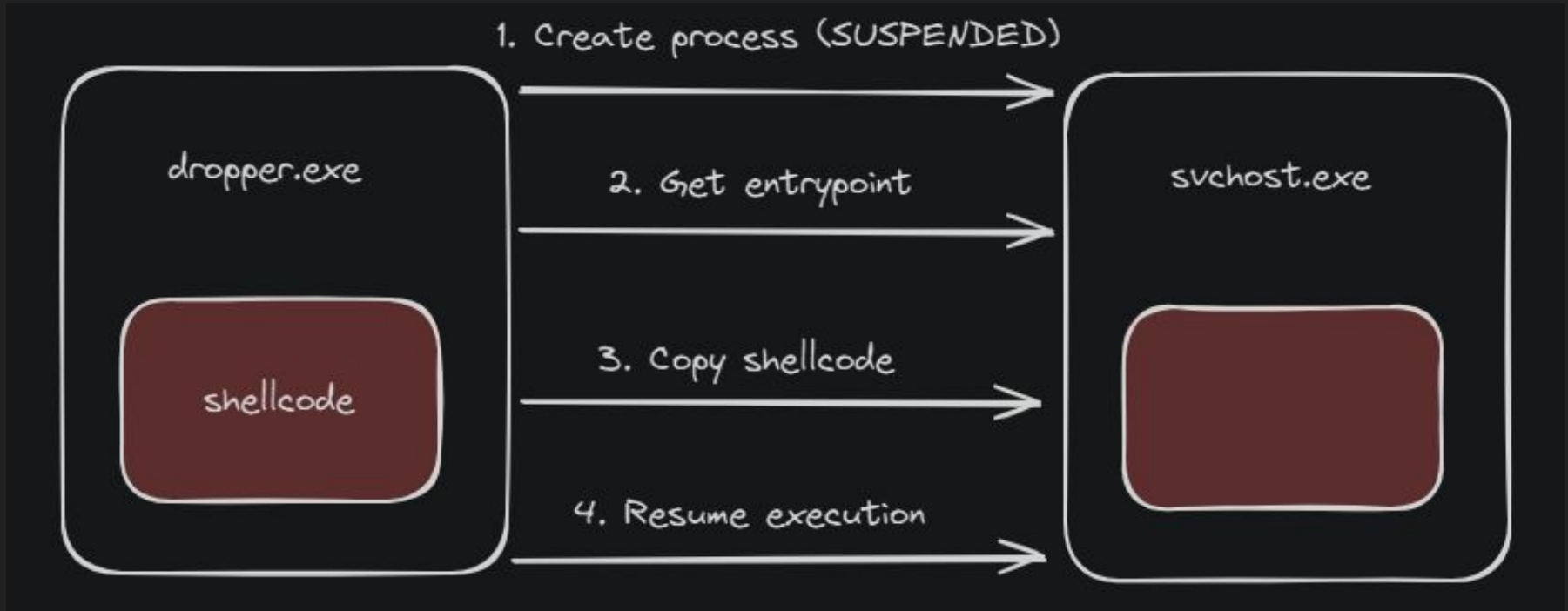
**TALK IS CHEAP**

**SHOW ME THE CODE**

# 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)<sup>264</sup> 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**

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/>