Malware Development 101

By Alice Climent-Pommeret

Summary

- What is an injection?
- Self injection
- Basic Remote injection
- DLL injection
- Thread hijacking
- MapView injection
- Bonus ? (if time… Hybrid injection)

About me

- Pentest and malware analysis at « French National Health Insurance »
- Star Wars fan
- Former baker
- ***NOT A DEV*** (you'll see…)
- @AliceCliment on Twitter / Hexe#5265 on Discord

What is an injection?

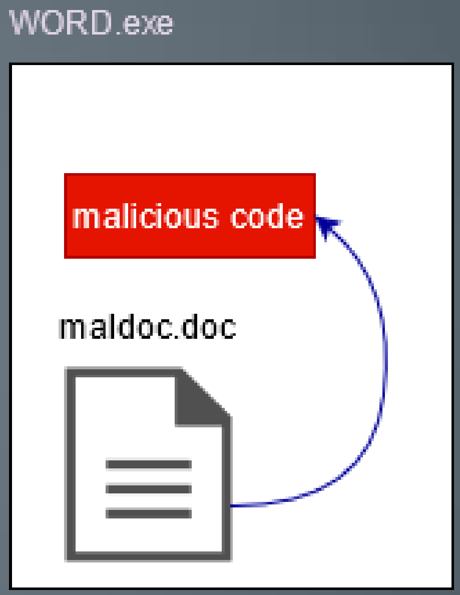
What is an injection?

“Process injection is a method of executing arbitrary code in the address space of a separate live process.

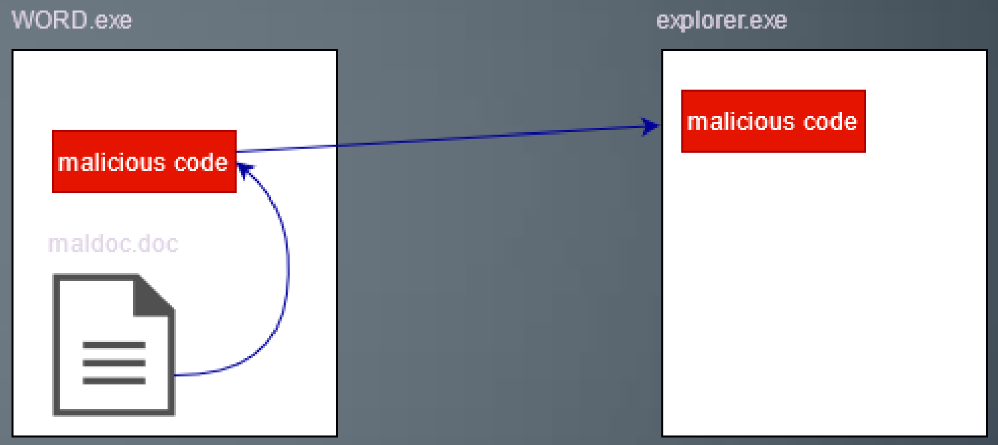
Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process”

https://attack.mitre.org/techniques/T1055/

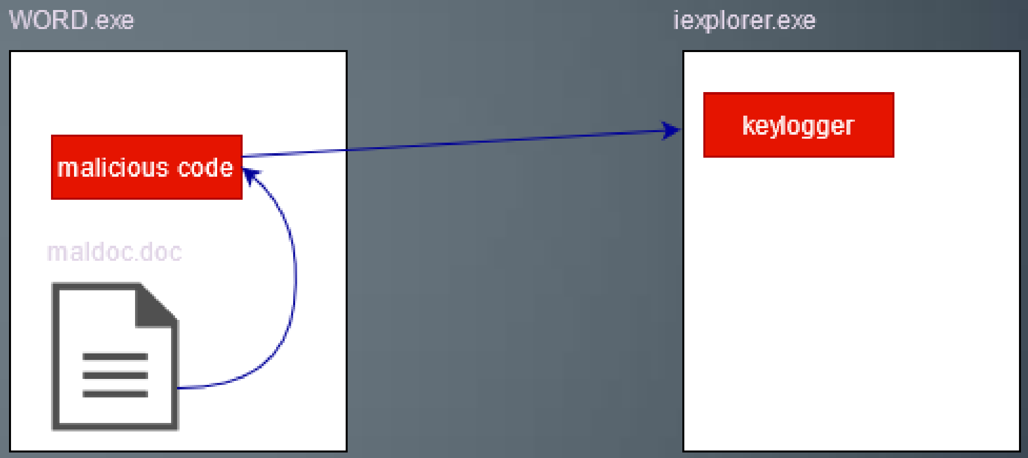
What is an injection?



What is an injection?



What is an injection?



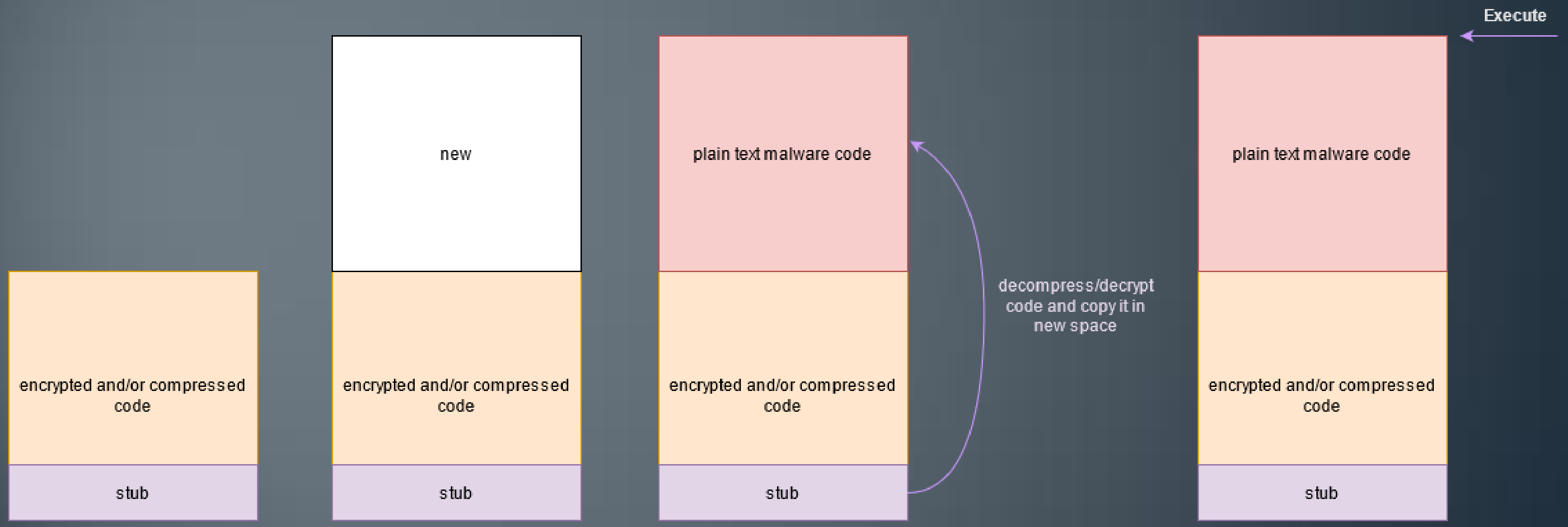
- What can be injected?
  - Shellcode
  - DLL
  - exe
  - Strings
  - Basically any data (but usually executable data)

Self Injection

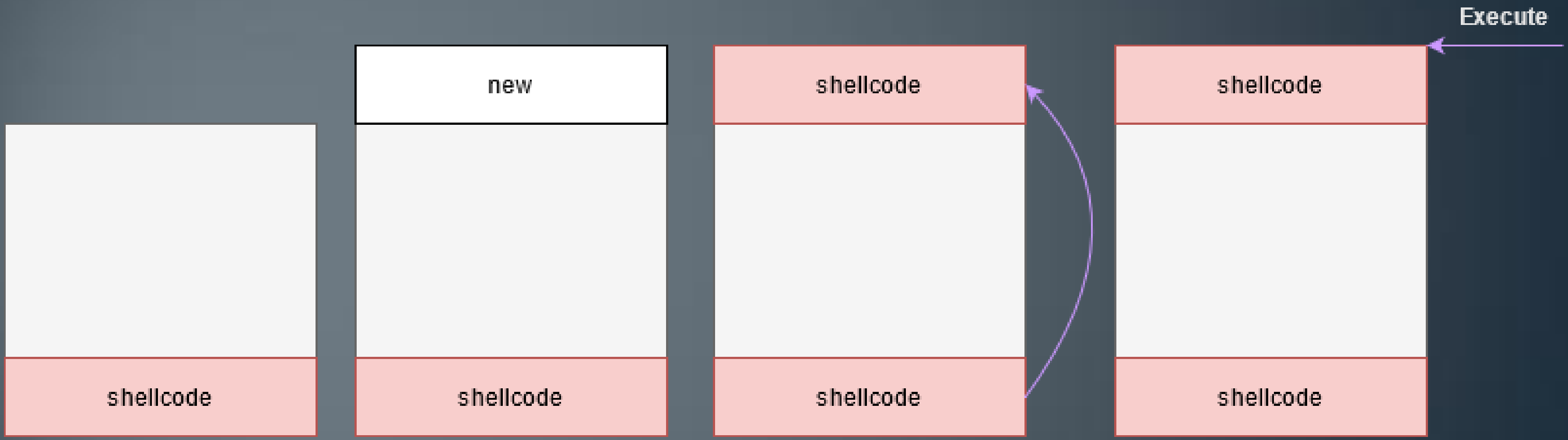
Self Injection

- Why ? Usually used in packed malware
- Common Windows API/function:
  - VirtualAlloc
  - VirtualProtect
  - CreateThread
  - memcpy
  - NtCreateThreadEx
  - NtProtectVirtualMemory
  - NtAllocationVirtualMemory
  - RtlMoveMemory
  - RtlCopyMemory

Unpacking


encrypted and/or compressed code
stub
new
encrypted and/or compressed code
stub
plain text malware code
encrypted and/or compressed code
stub
decompress/decrypt code and copy it in new space
Execute
plain text malware code
encrypted and/or compressed code
stub

Self Injection

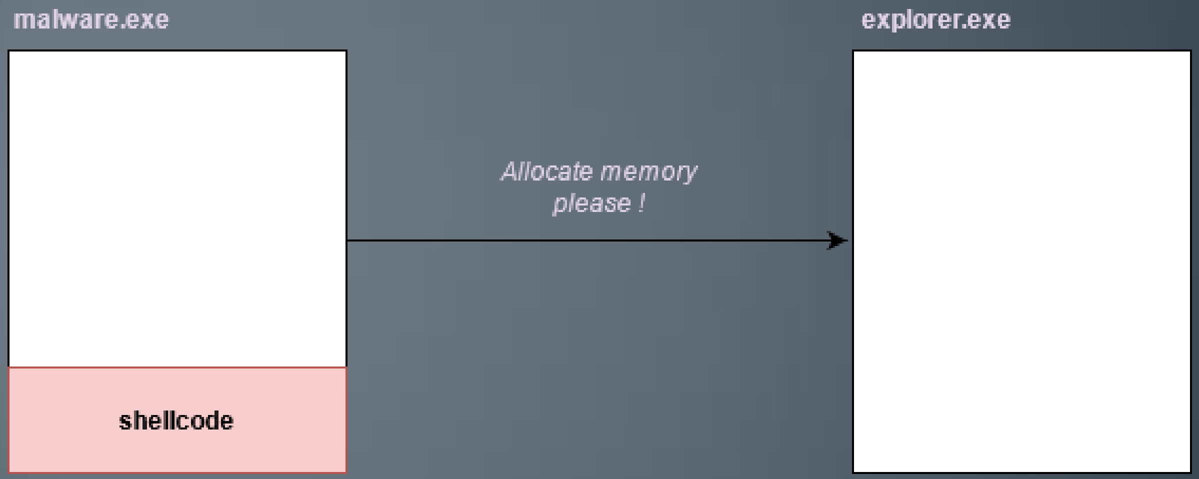


Basic Remote Injection

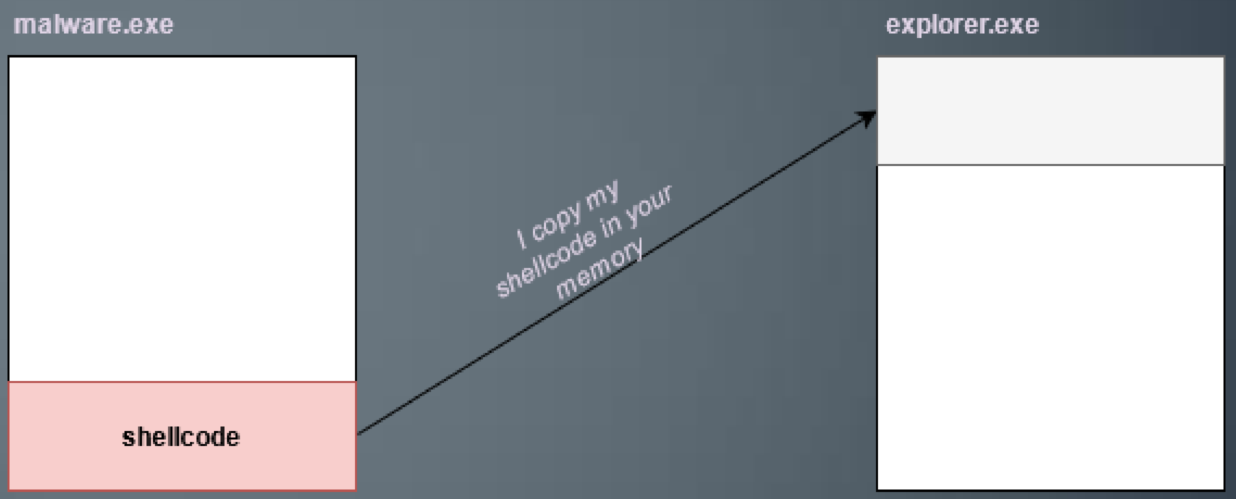
Common Windows API/function:

- VirtualAllocEx
- OpenProcess
- NtOpenProcess
- VirtualProtectEx
- CreateRemoteThread
- WriteProcessMemory
- NtCreateThreadEx
- NtProtectVirtualMemory
- NtAllocationVirtualMemory
- NtWriteVirtualMemory

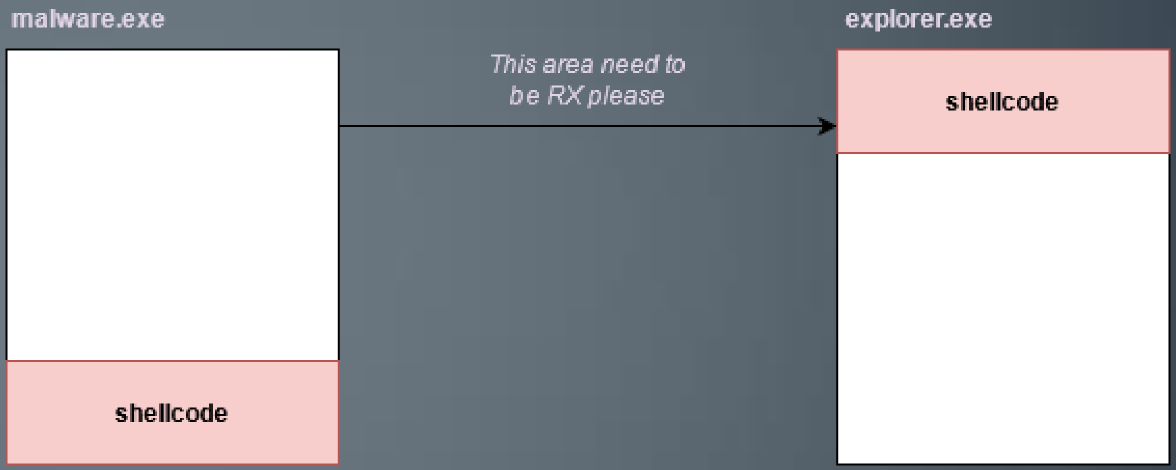
Remote Injection



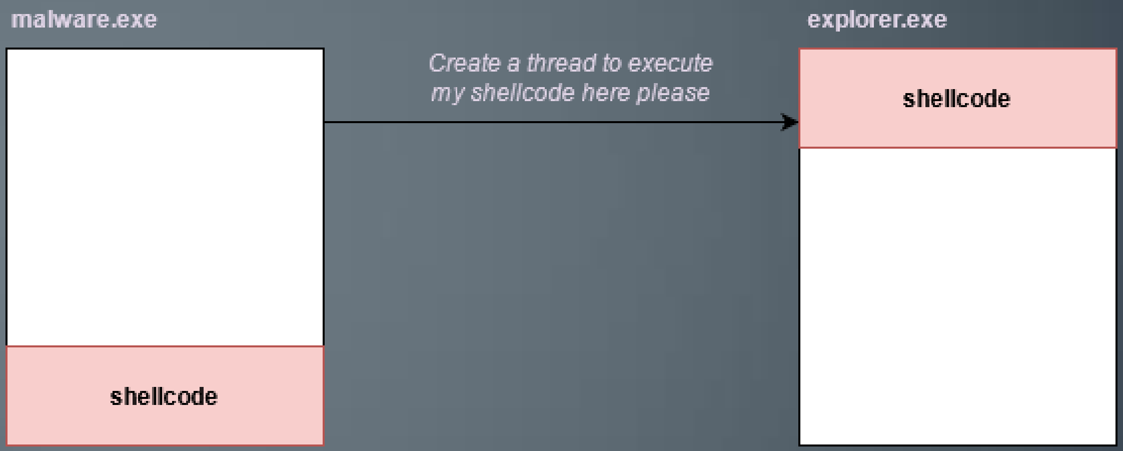
Remote Injection



Remote Injection



Remote Injection



DLL Injection

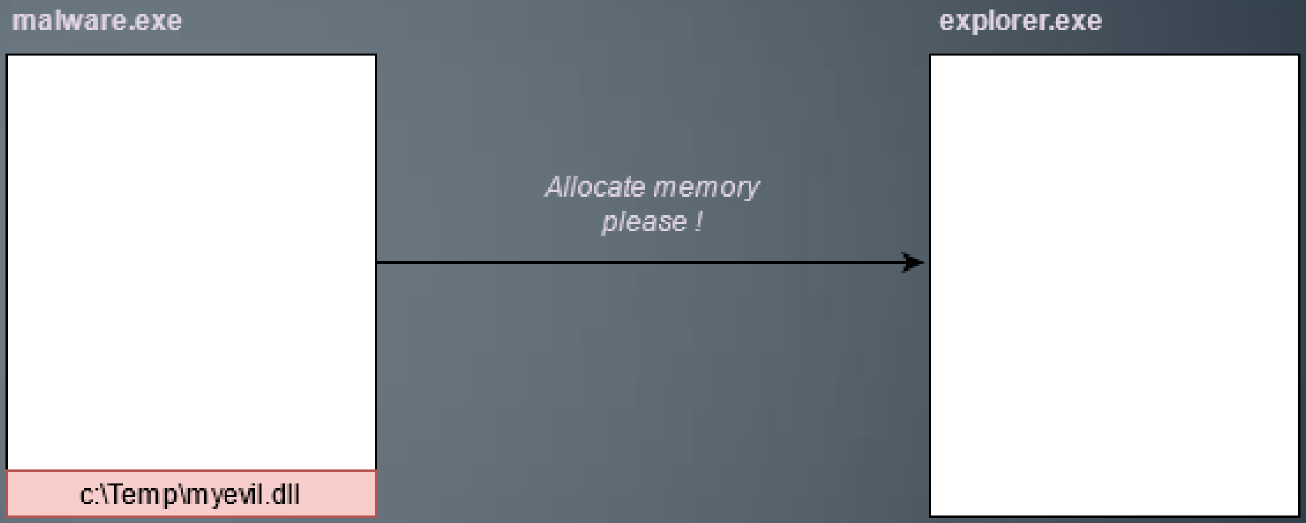
Benefit(s)

- No shellcode/malicious code in the first stage executable
- Can look legit in the remote process

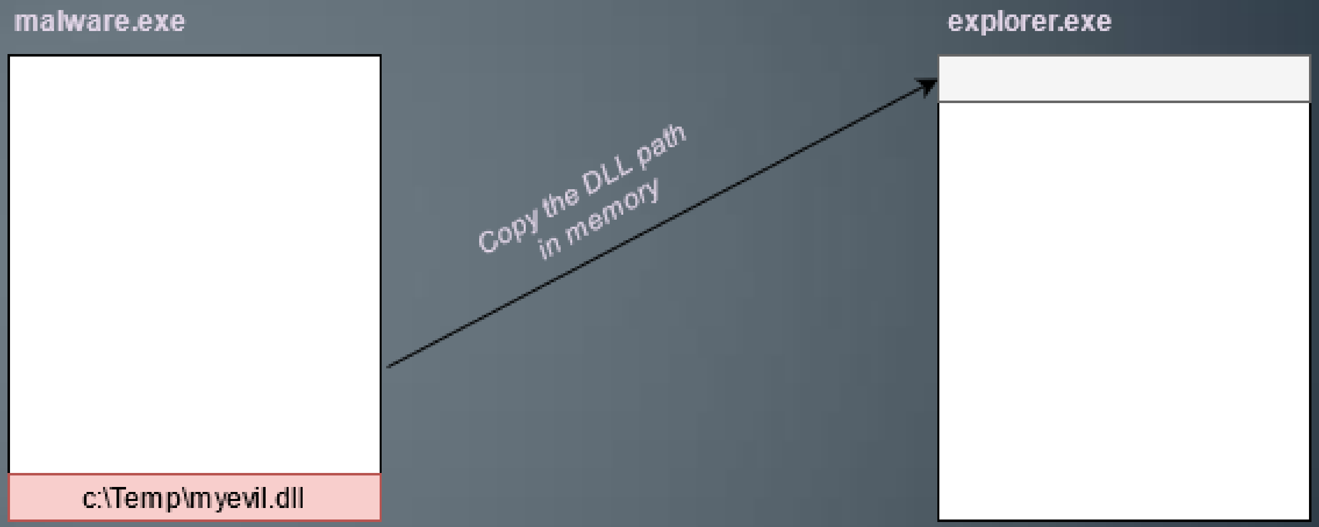
Common Windows API/function:

- VirtualAllocEx
- OpenProcess
- NtOpenProcess
- CreateRemoteThread
- WriteProcessMemory
- NtCreateThreadEx
- NtAllocationVirtualMemory
- NtWriteVirtualMemory

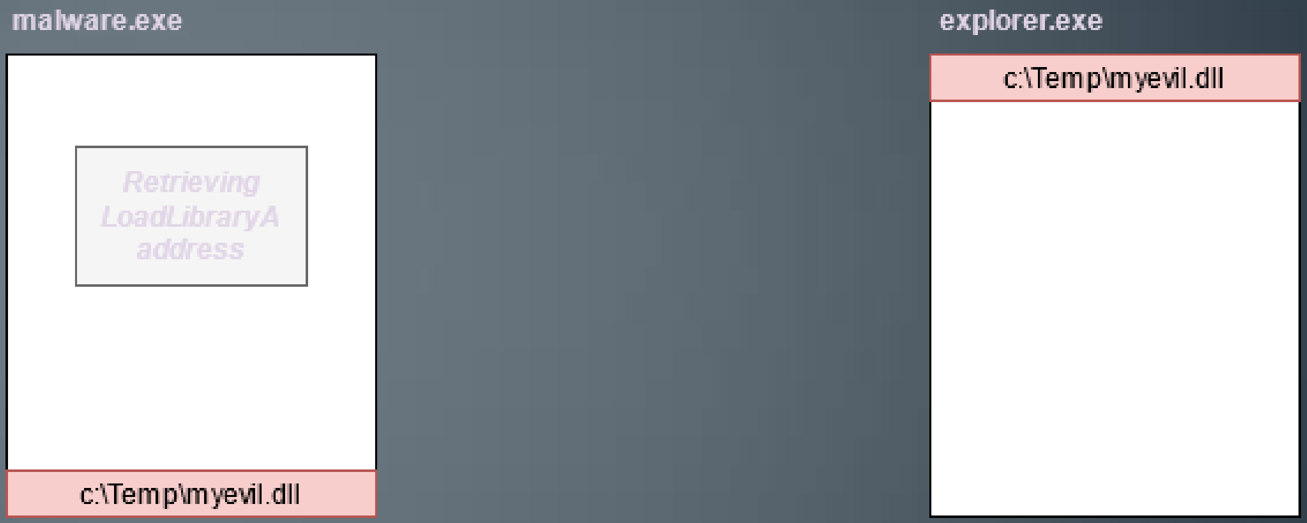
DLL Injection



DLL Injection



DLL Injection



malware.exe

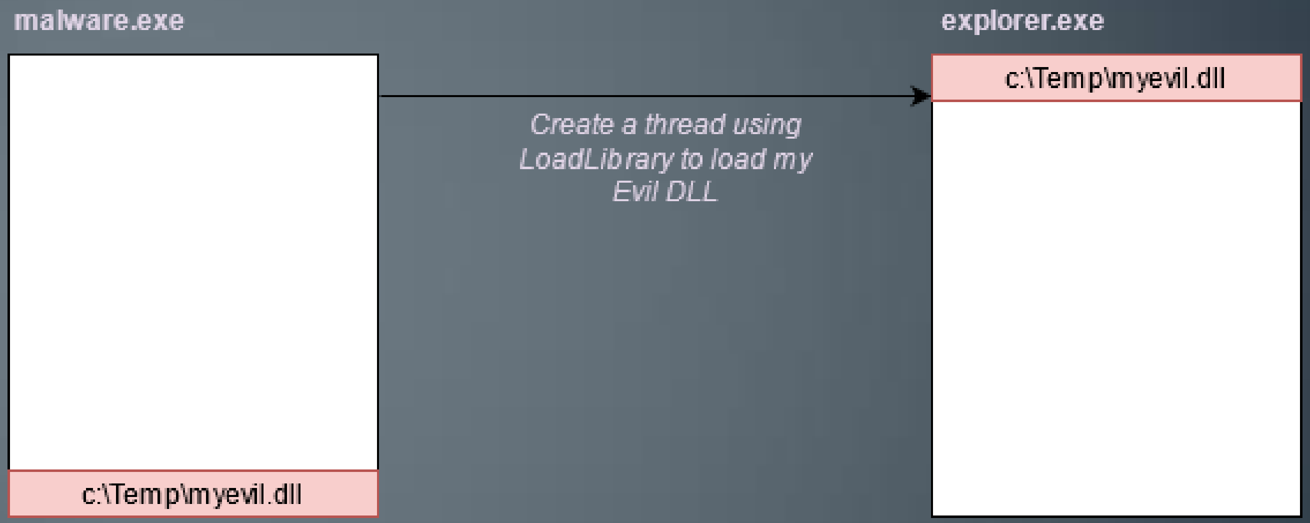
Retrieving LoadLibraryA address

c:\Temp\myevil.dll

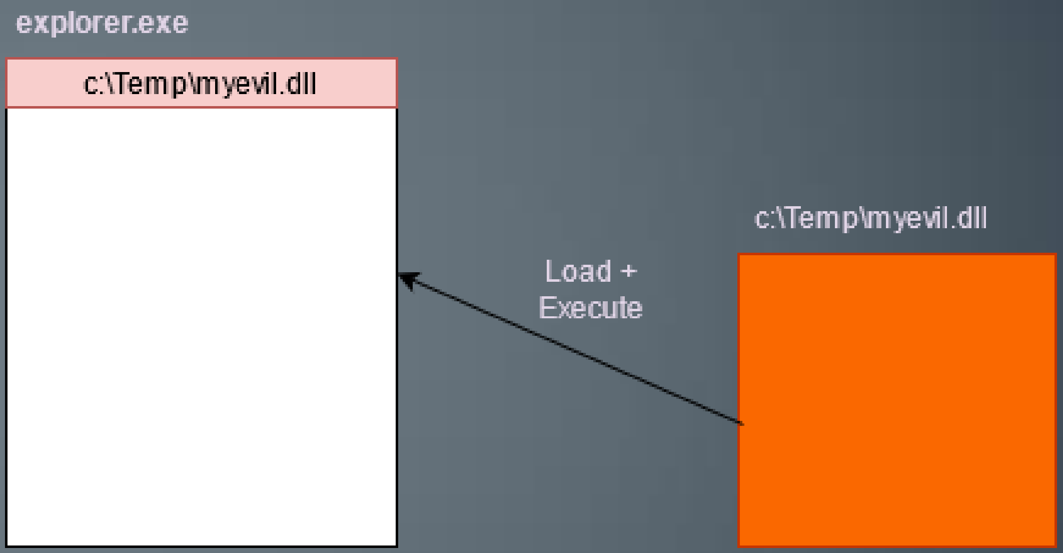
explorer.exe

c:\Temp\myevil.dll

DLL Injection



DLL Injection



Thread Hijacking

Benefit(s)

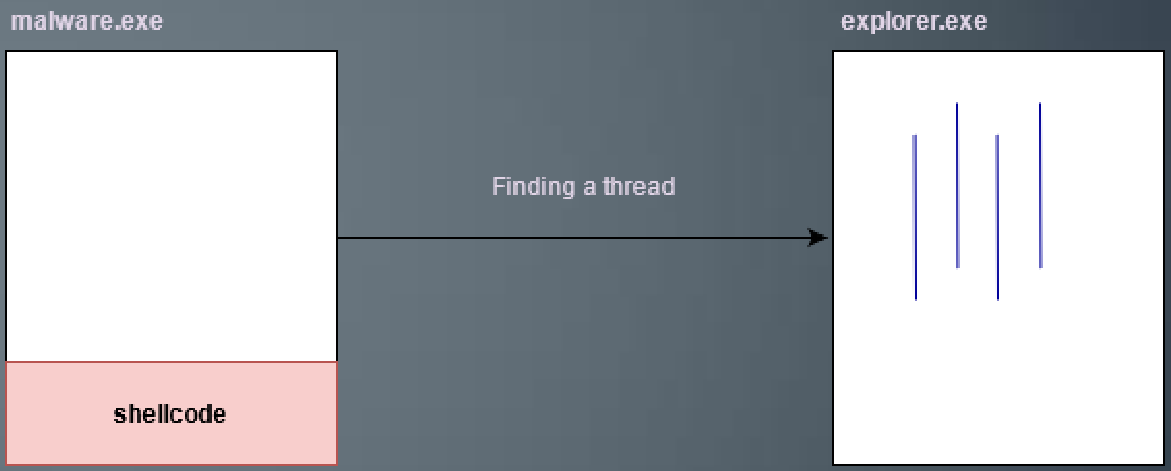
- No use of the Windows API « CreateRemoteThread » or « NtCreateThreadEx » (can be monitored by security product)

Common Windows API/function:

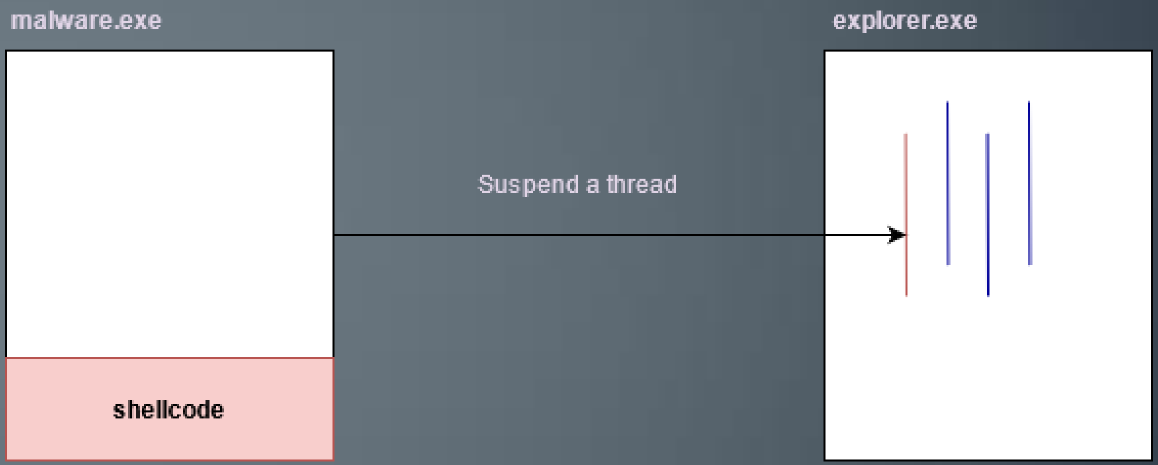
- VirtualAllocEx
- OpenProcess
- NtOpenProcess
- WriteProcessMemory
- NtAllocationVirtualMemory
- NtWriteVirtualMemory

- SuspendThread
- NtSuspendThread
- GetThreadContext
- NtGetContextThread
- SetThreadContext
- NtSetContextThread
- ResumeThread
- NtResumeThread

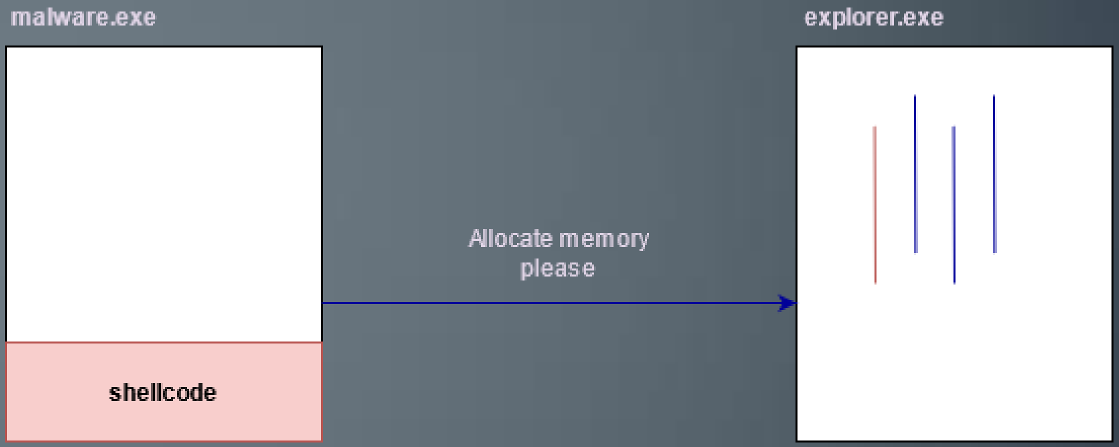
Thread Hijacking



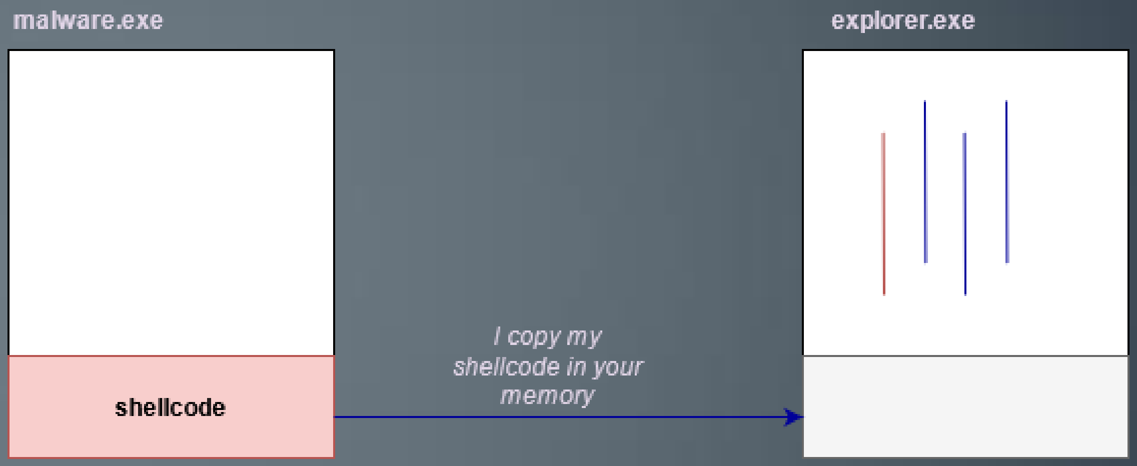
Thread Hijacking



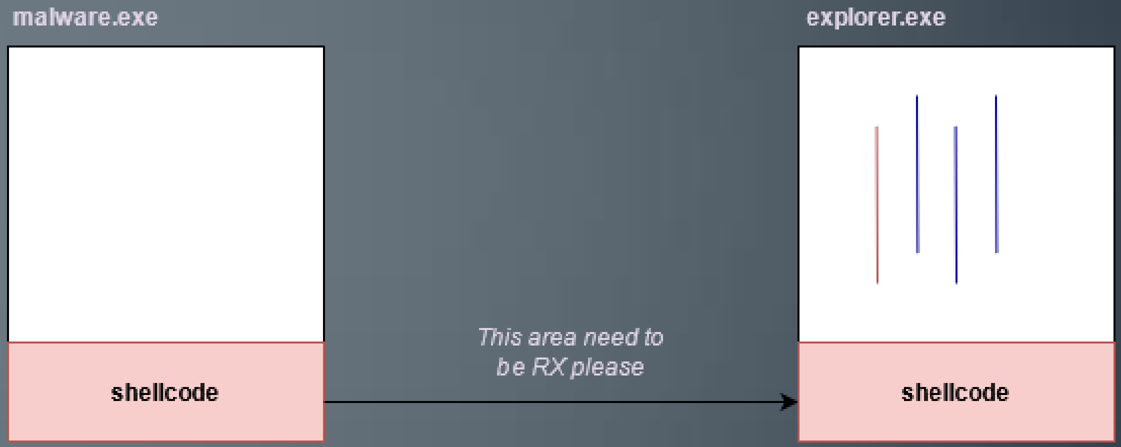
Thread Hijacking



Thread Hijacking



Thread Hijacking



malware.exe

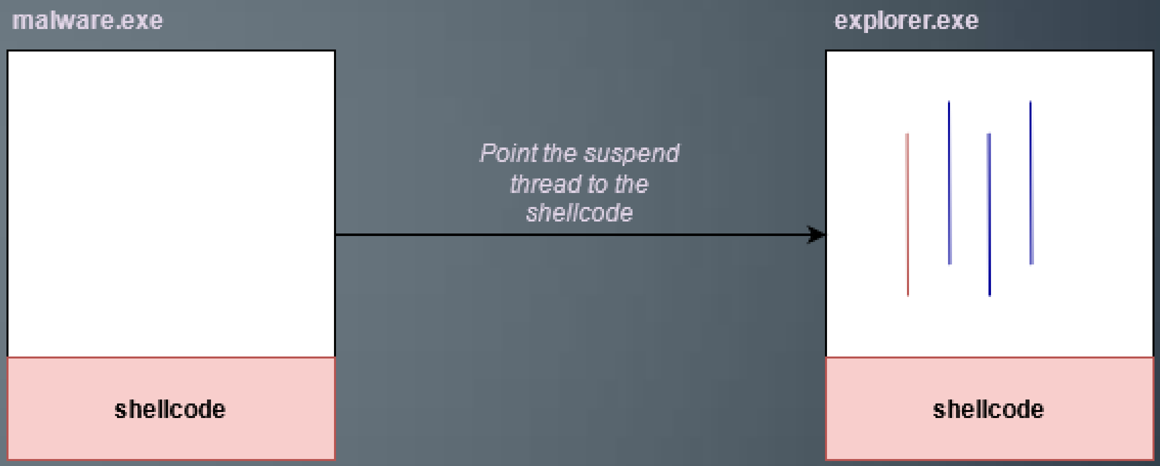
shellcode

This area need to be RX please

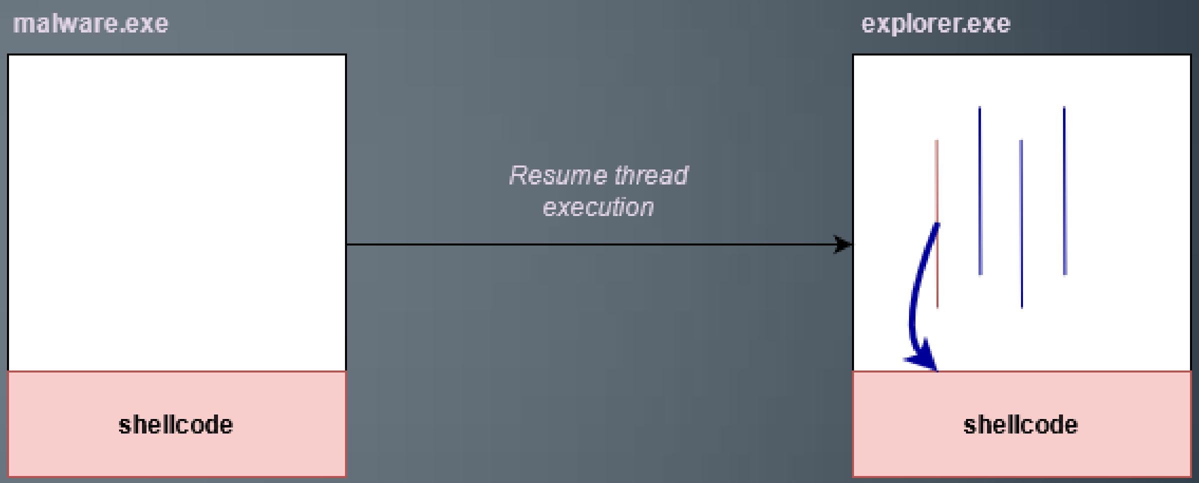
explorer.exe

shellcode

Thread Hijacking



Thread Hijacking



MapView Injection

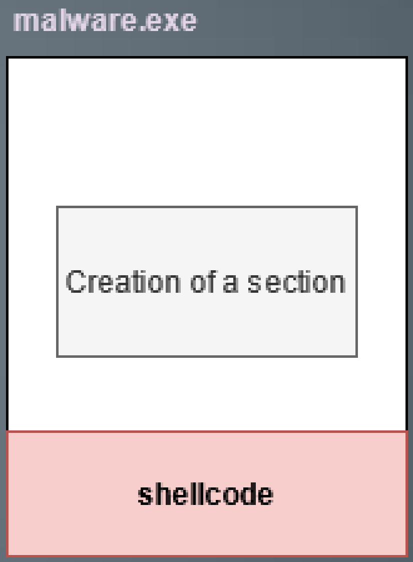
Benefit(s)

- No use of the Windows API « WriteProcessMemory » or « NtWriteVirtualMemory » (can be monitored by security product)

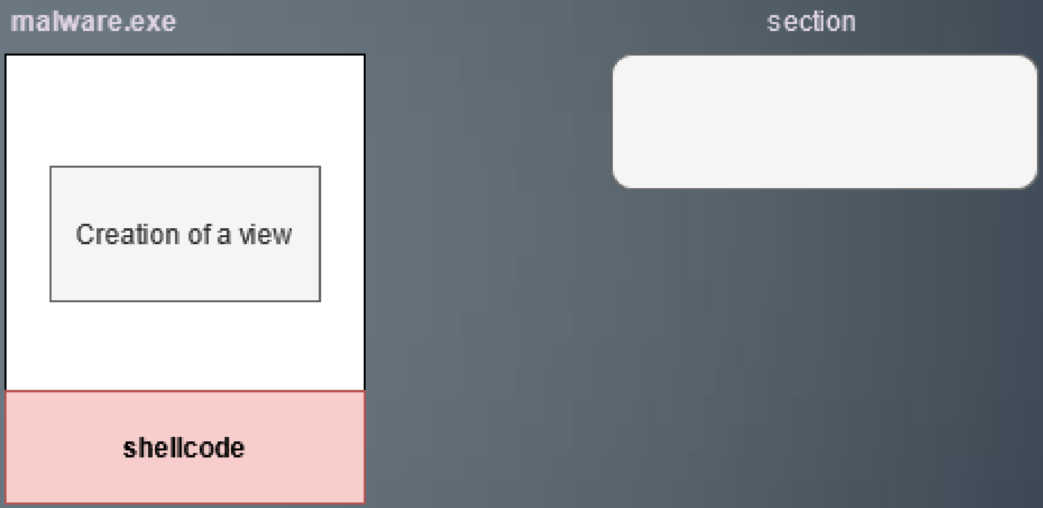
Common Windows API/function:

- OpenProcess
- NtOpenProcess
- CreateRemoteThread
- NtCreateThreadEx
- NtCreateSection
- NtMapViewOfSection

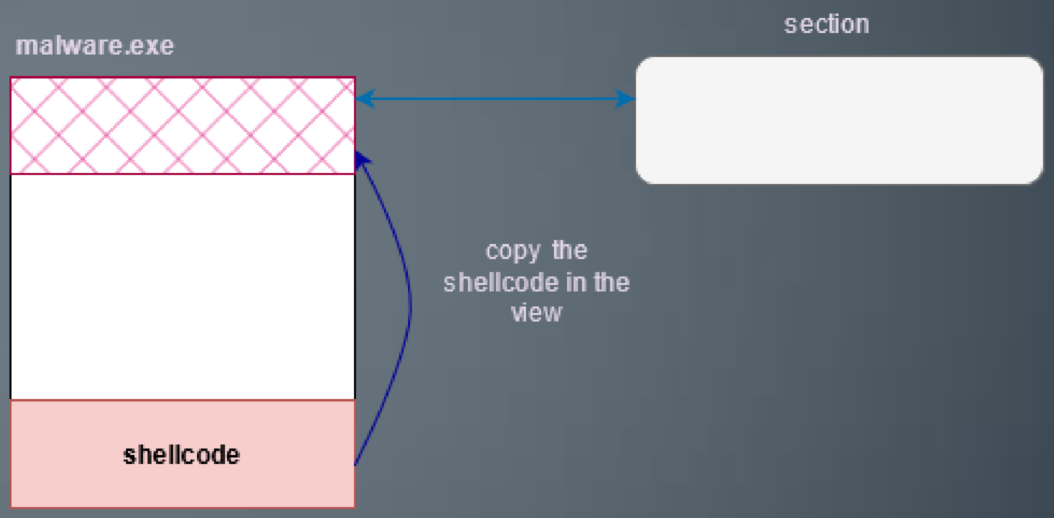
MapView Injection



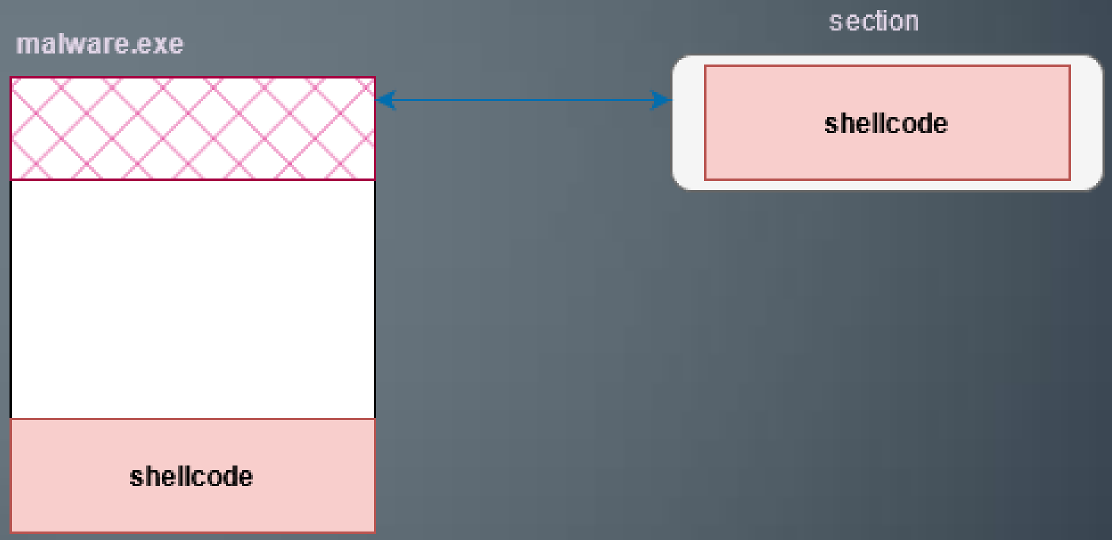
MapView Injection



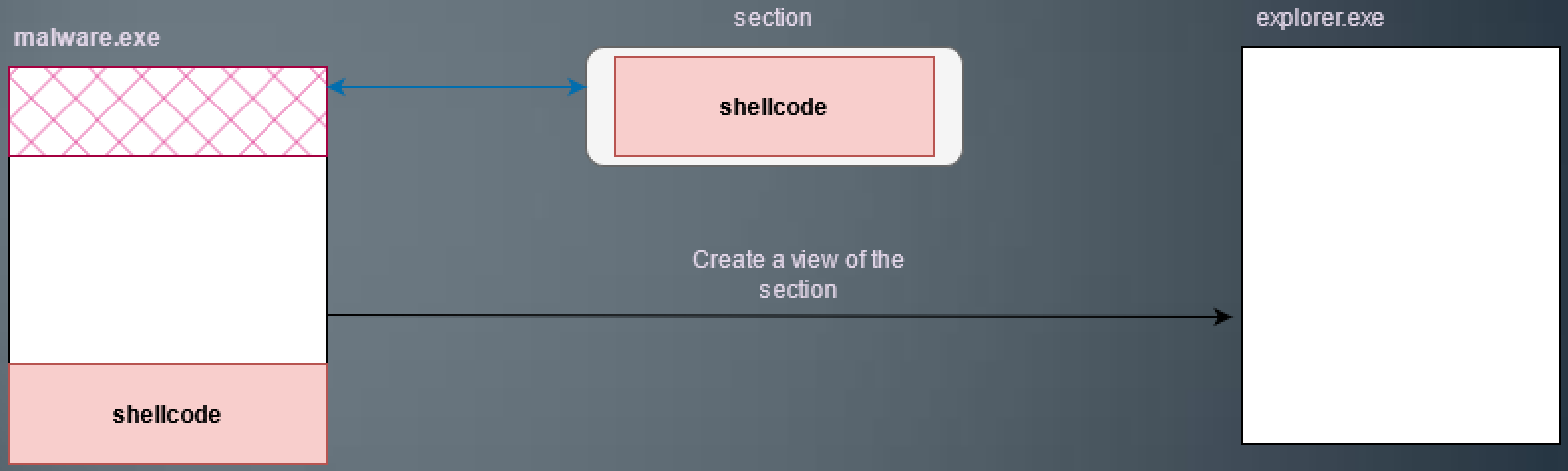
MapView Injection



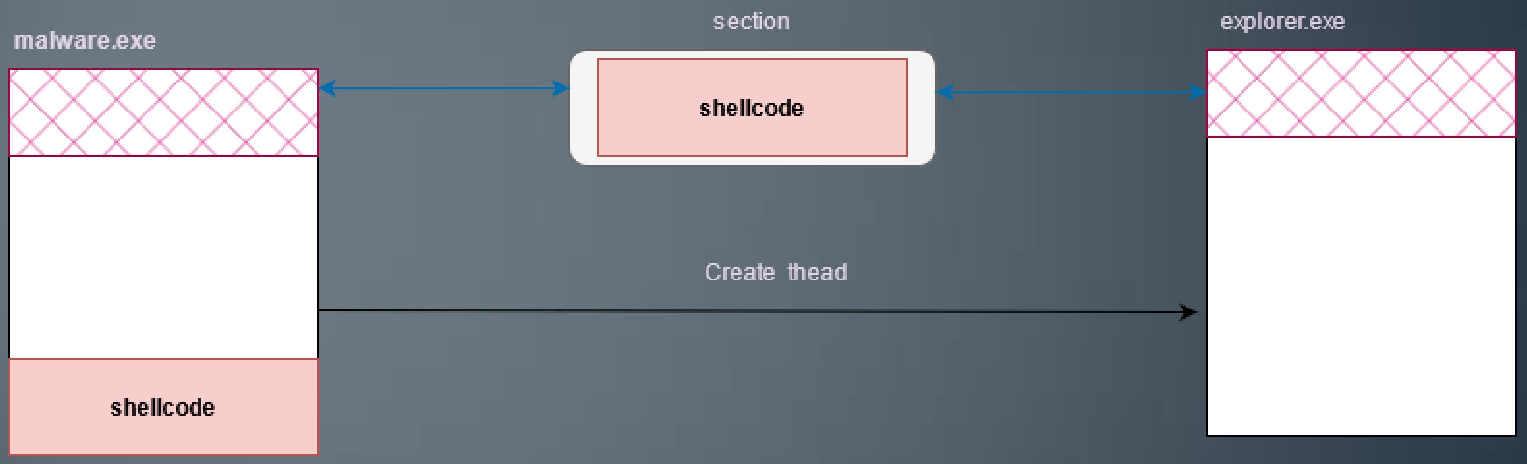
MapView Injection



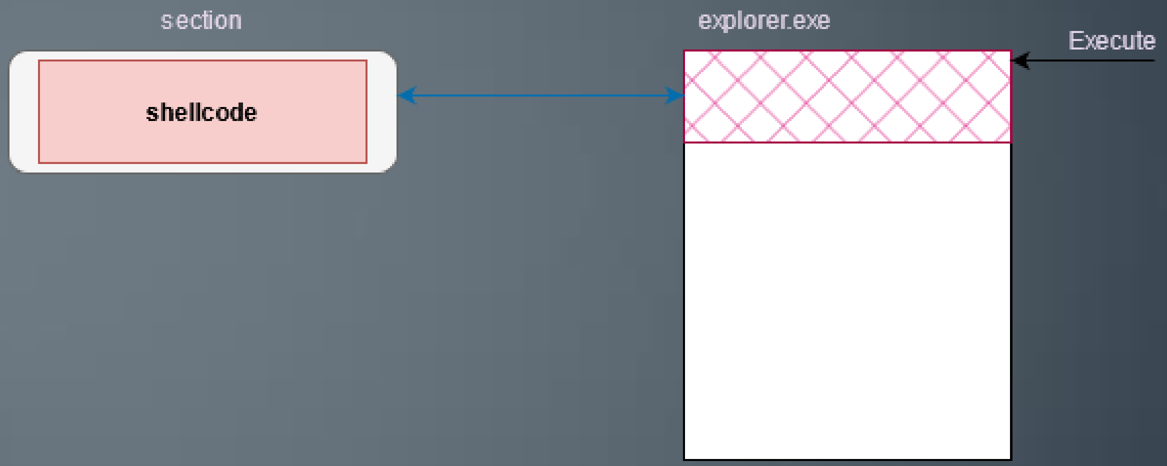
MapView Injection



MapView Injection



MapView Injection



Bonus: Hybrid Injection

Hybrid Injection

- Not an « official » injection technique
- Just a mix of Thread Hijacking and MapView injection
- Made it up just for this workshop

Benefit(s)

- No use of the Windows API « WriteProcessMemory » or « NtWriteVirtualMemory » (can be monitored by security product)
- No use of the Windows API « CreateRemoteThread » or « NtCreateThreadEx » (can be monitored by security product)

If you want to learn more…

- https://institute.sektor7.net/ (Fee-based online courses, awesome)
- https://github.com/vxunderground/VX-API (free, awesome, lots of interesting code)
- https://www.vx-underground.org/windows.html (free, awesome, malware research papers)
- https://github.com/hasherezade/ (free, awesome, if you are looking for a specific process injection technique code, it's probably here)
- https://hshrzd.wordpress.com/ (her blog !)

If you want to play hide and seek

- https://github.com/hasherezade/pe-sieve

More about process injection

- https://www.youtube.com/watch?v=xewv122qxnk
- https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf
- https://www.vx-underground.org/windows.html#process_injection

That's all Folks!