

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

The background of the slide features a series of thin, vertical, light blue lines of varying heights and positions, creating a textured, rain-like effect. A solid teal horizontal band spans the width of the slide, positioned in the lower half. The text "What is an injection?" is centered within this band.

What is an injection?

What is an injection?

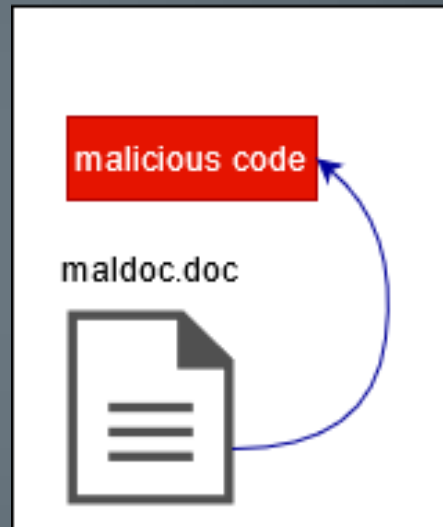
“Process injection is a method of executing arbitrary code in the address space of a separate live process.

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”

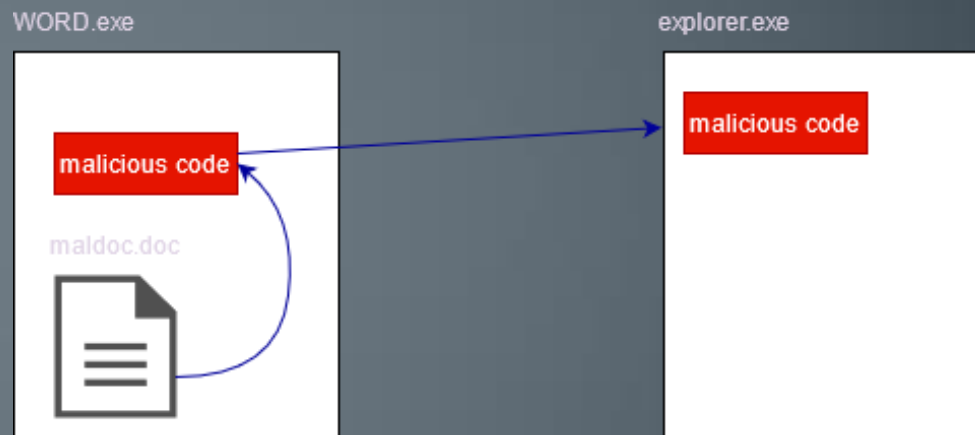
<https://attack.mitre.org/techniques/T1055/>

What is an injection?

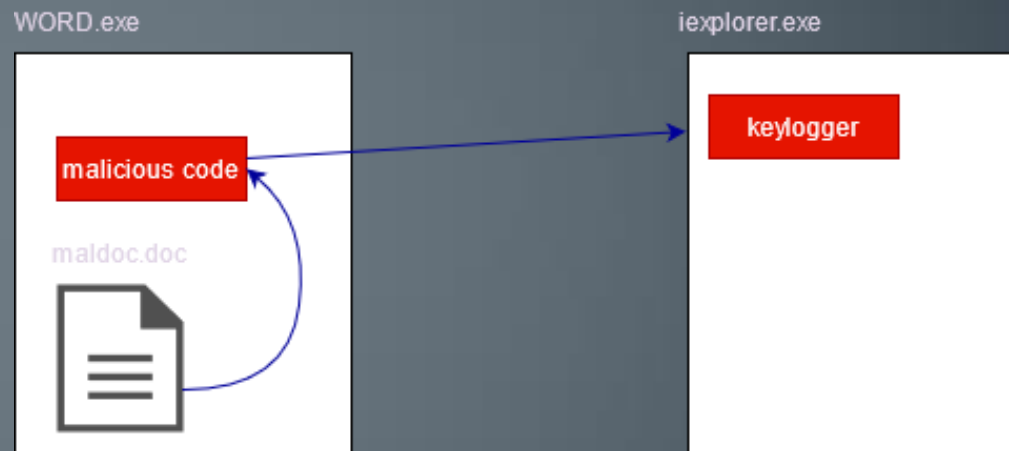
WORD.exe



What is an injection?



What is an injection?



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

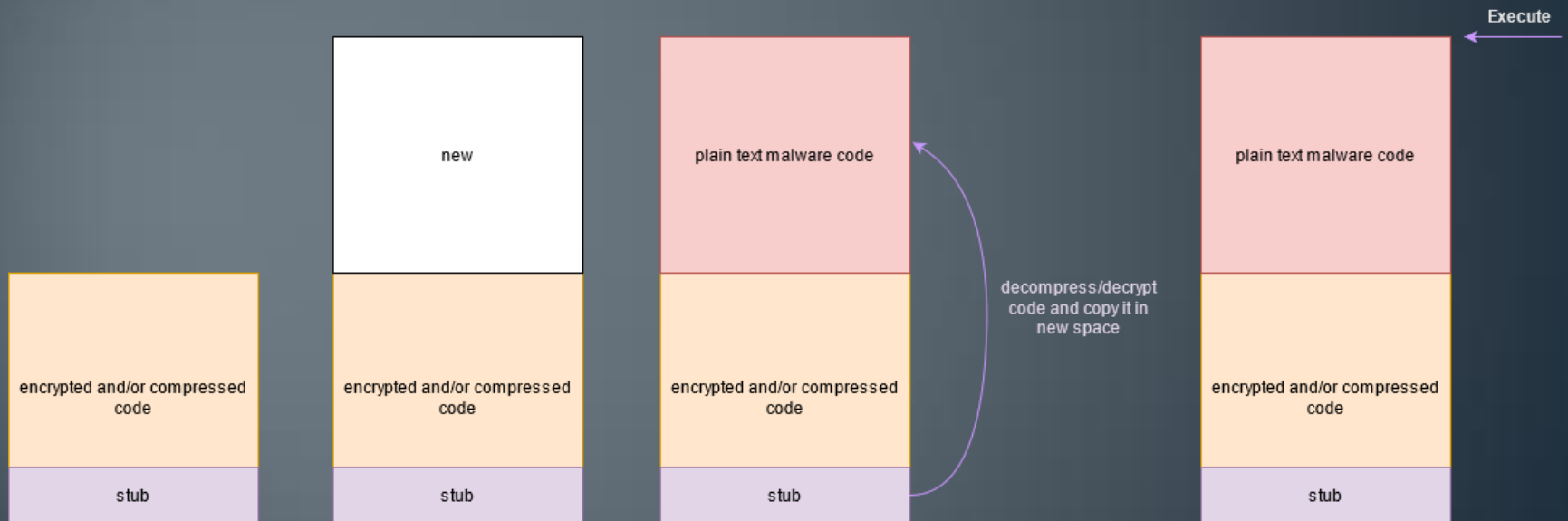
The background of the slide features a series of thin, vertical, slightly wavy lines in a light blue-grey color against a light grey gradient. A solid teal horizontal band spans the width of the slide, positioned in the lower half. The text 'Self Injection' is written in a white, bold, sans-serif font within this band.

Self Injection

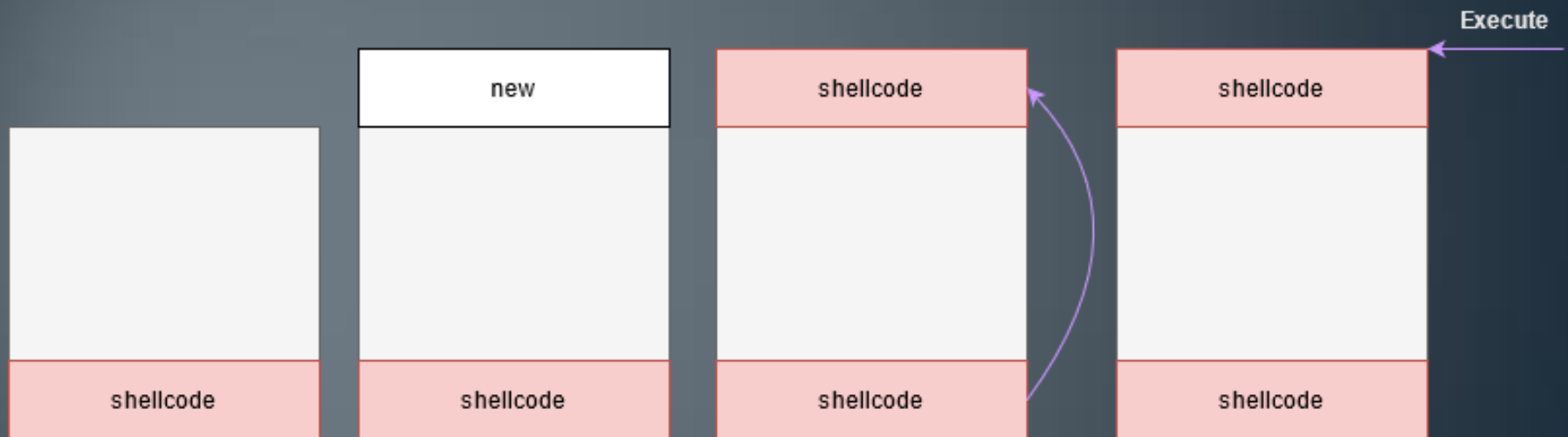
Self Injection

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

Unpacking



Self Injection



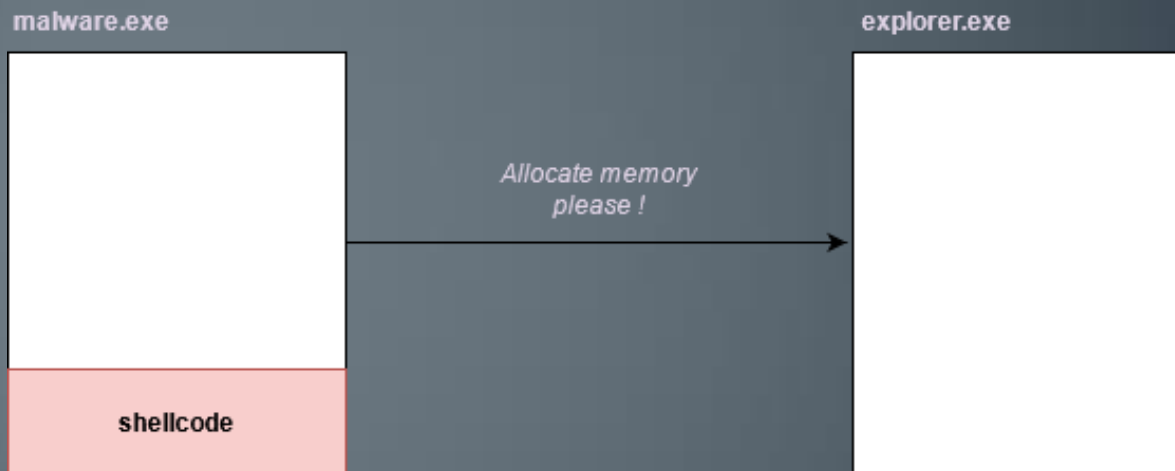
The background of the slide features a series of vertical lines in various shades of blue and grey, creating a textured, rain-like effect. A solid dark blue horizontal band spans the width of the slide, serving as a backdrop for the title text.

Basic Remote Injection

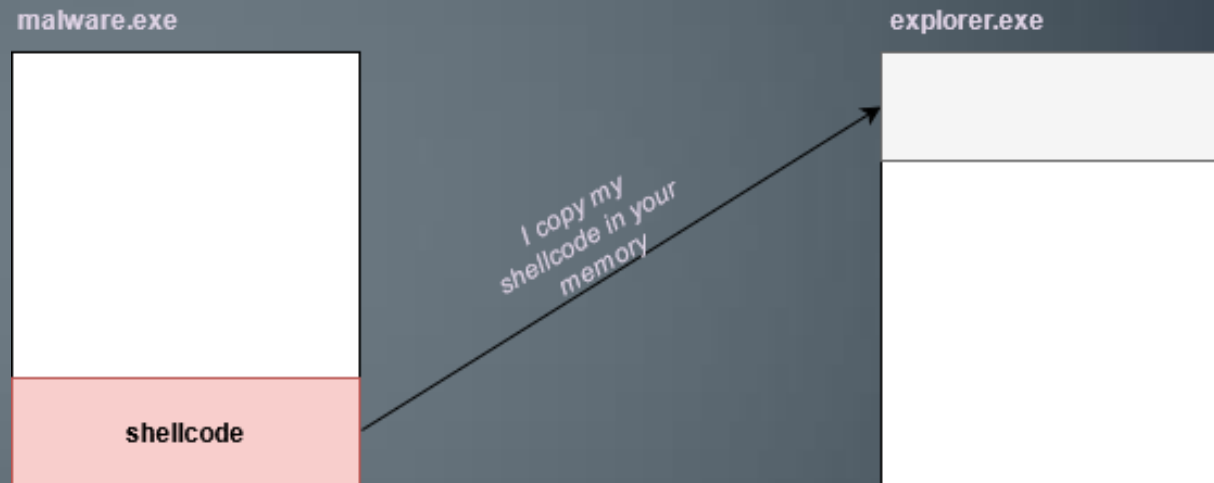
Common Windows API/function:

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

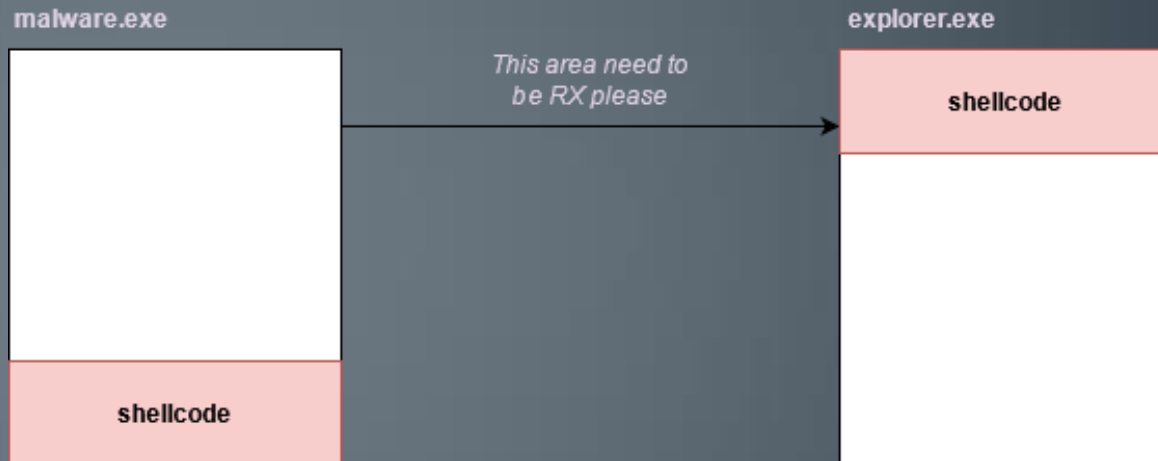
Remote Injection



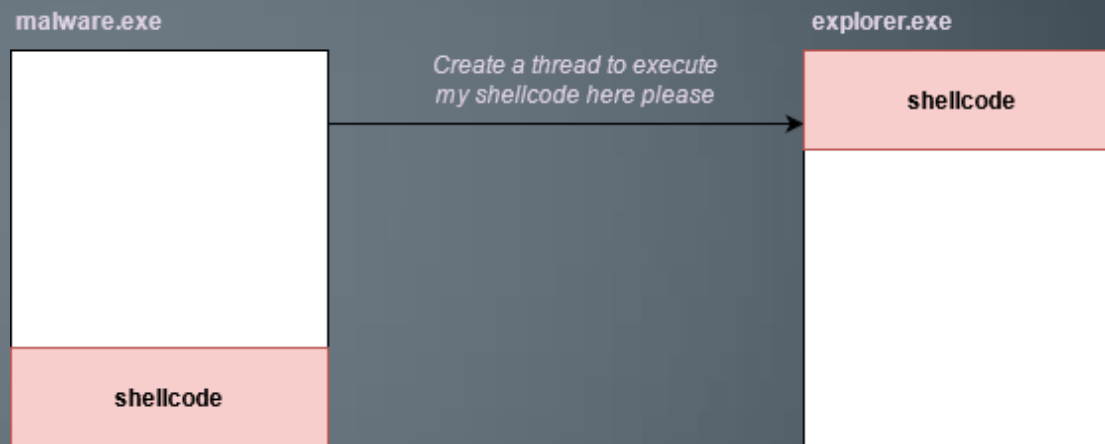
Remote Injection



Remote Injection



Remote Injection



The background of the slide features a pattern of thin, vertical, slightly wavy lines in a light blue-grey color against a darker grey background. A solid teal horizontal bar spans the width of the slide, positioned below the patterned area. The text 'DLL Injection' is written in white with a thin black outline, located in the lower-left portion of the teal bar.

DLL Injection

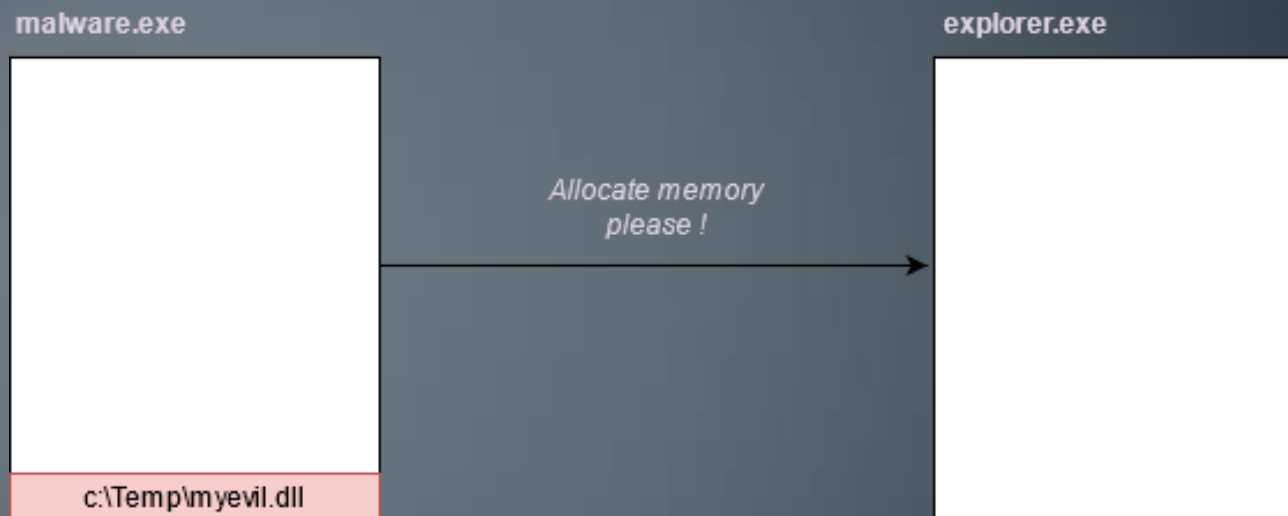
Benefit(s)

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

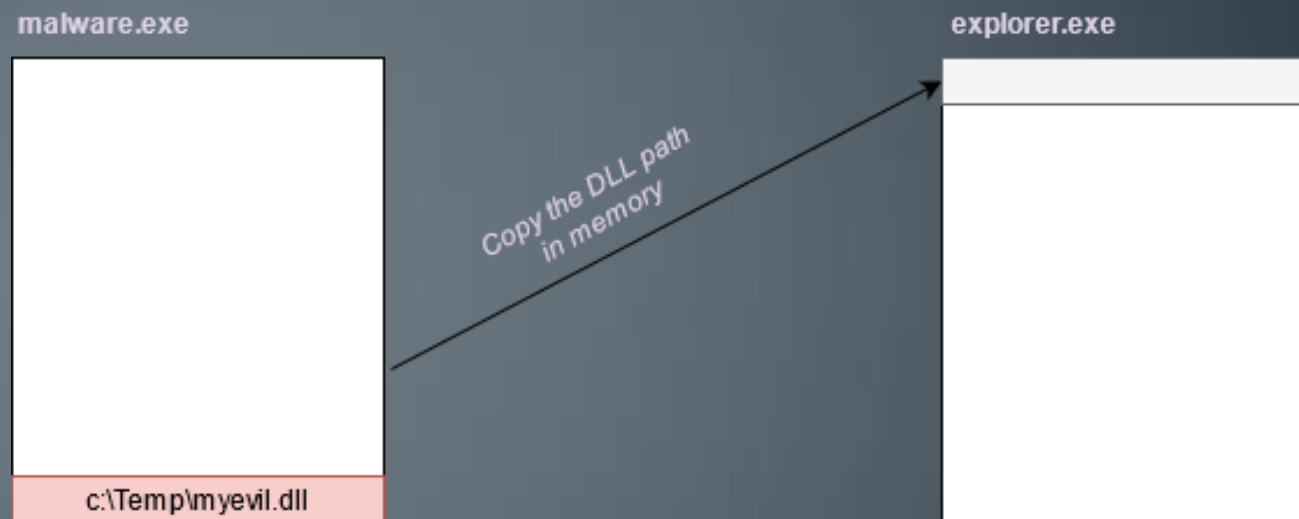
Common Windows API/function:

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

DLL Injection

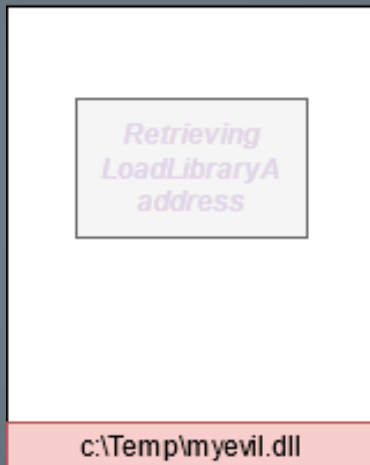


DLL Injection

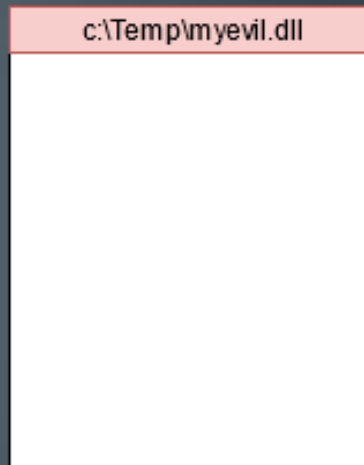


DLL Injection

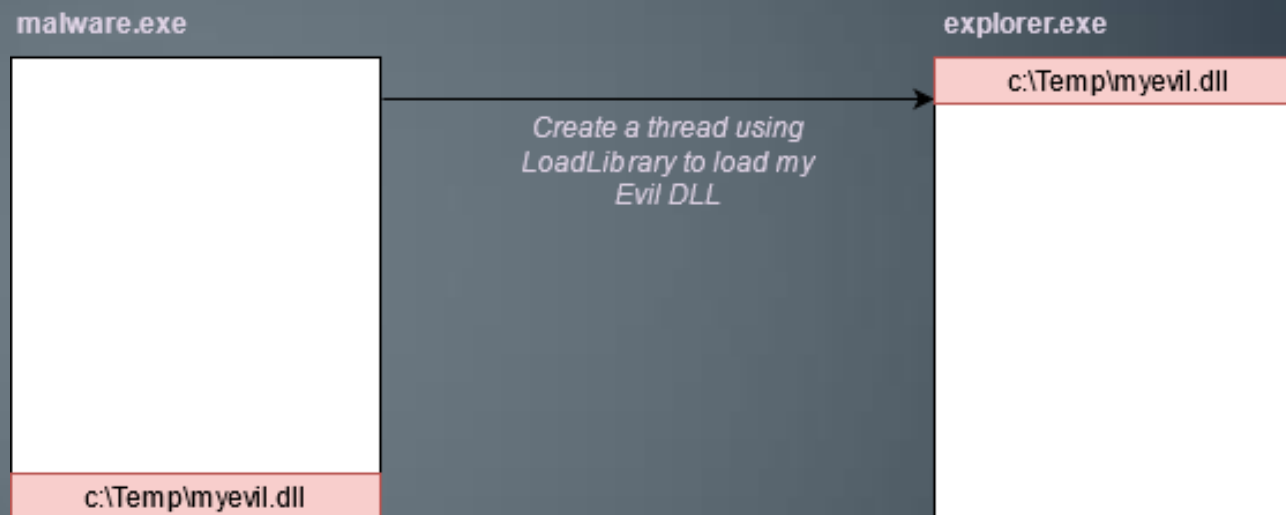
malware.exe



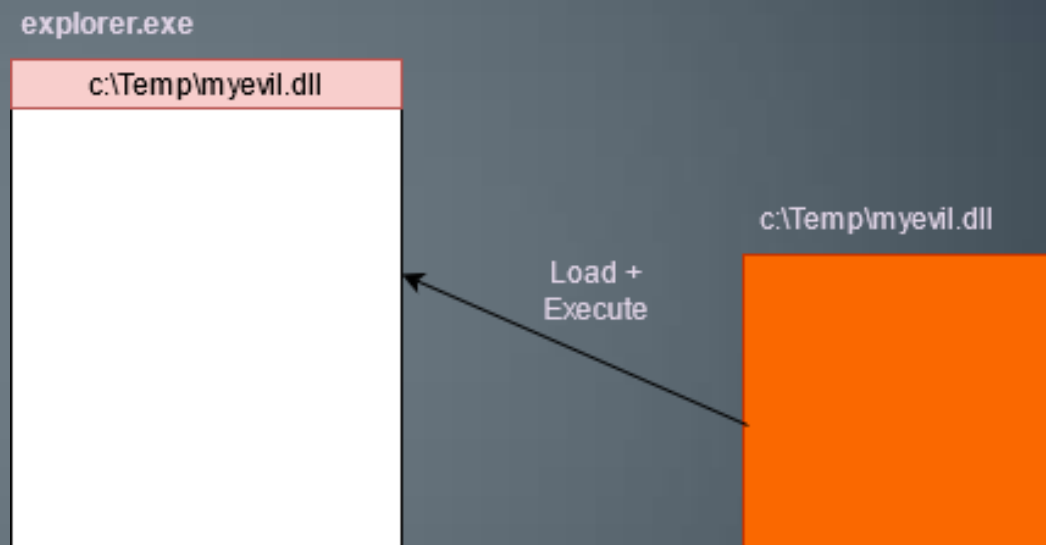
explorer.exe



DLL Injection



DLL Injection



The background features a series of thin, vertical, slightly wavy lines in a light blue-grey color against a light grey gradient. A solid teal horizontal band spans the width of the image, positioned in the lower half. The title 'Thread Hijacking' is written in white text with a thin black outline, centered within this teal band.

Thread Hijacking

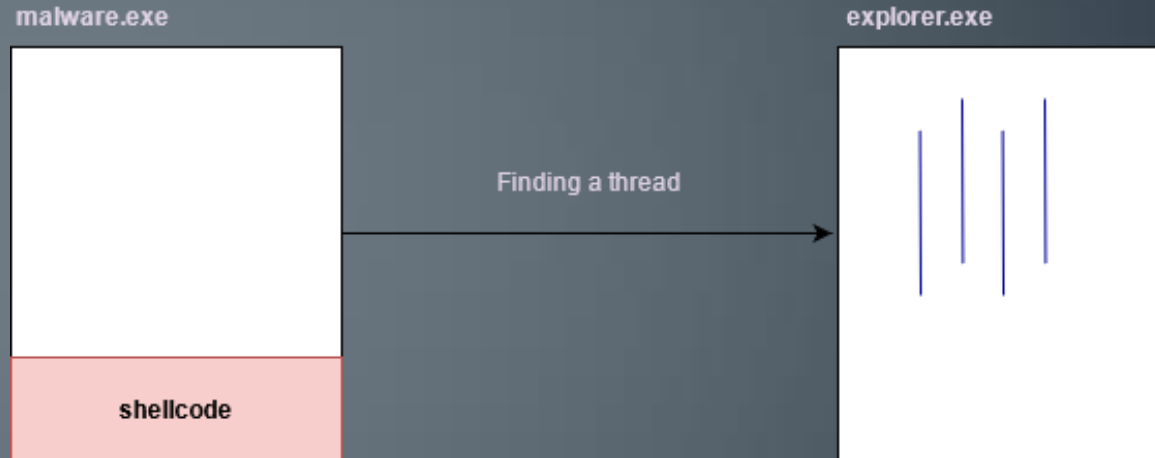
Benefit(s)

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

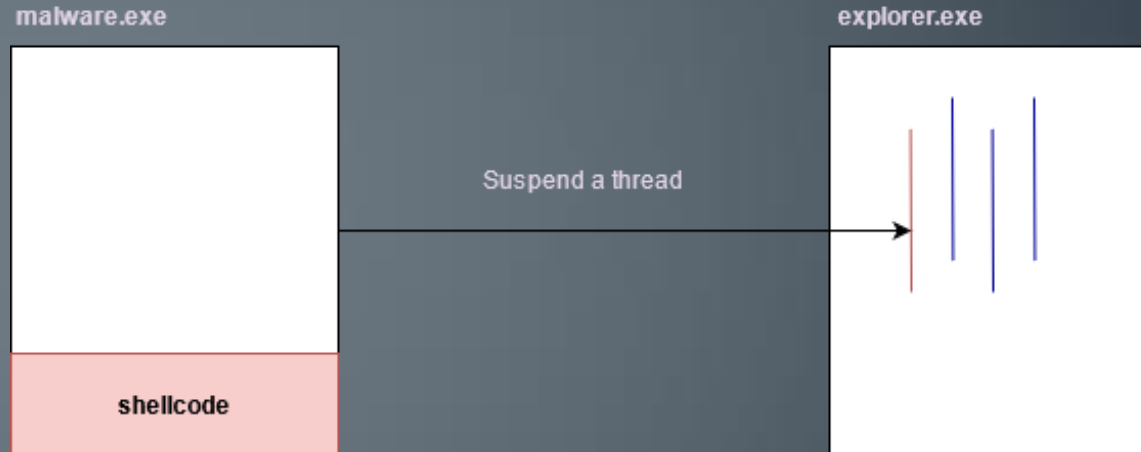
Common Windows API/function:

- VirtualAllocEx
- OpenProcess
- NtOpenProcess
- WriteProcessMemory
- NtAllocationVirtualMemory
- NtWriteVirtualMemory
- SuspendThread
- NtSuspendThread
- GetThreadContext
- NtGetContextThread
- SetThreadContext
- NtSetContextThread
- ResumeThread
- NtResumeThread

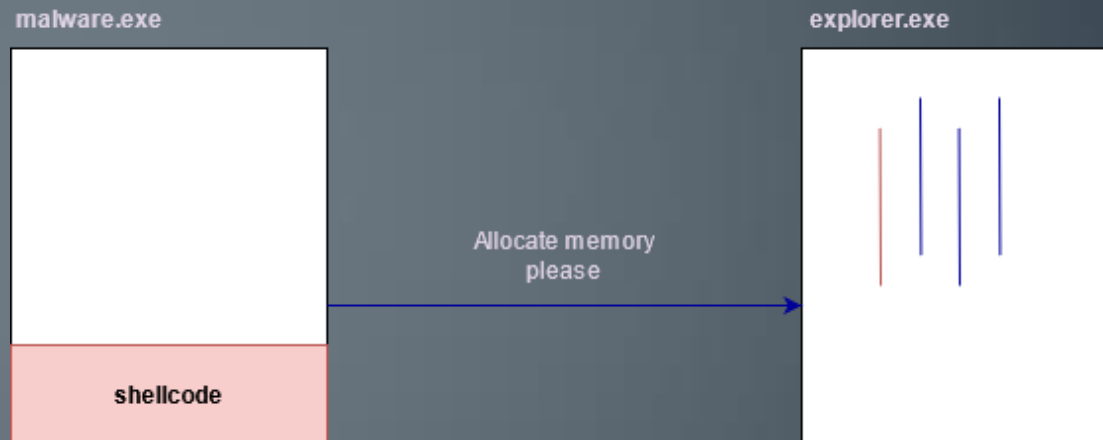
Thread Hijacking



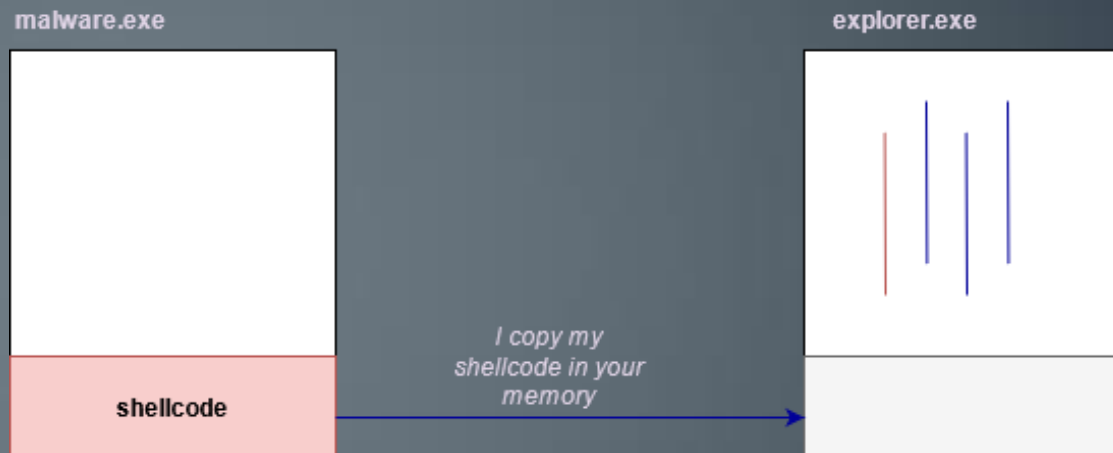
Thread Hijacking



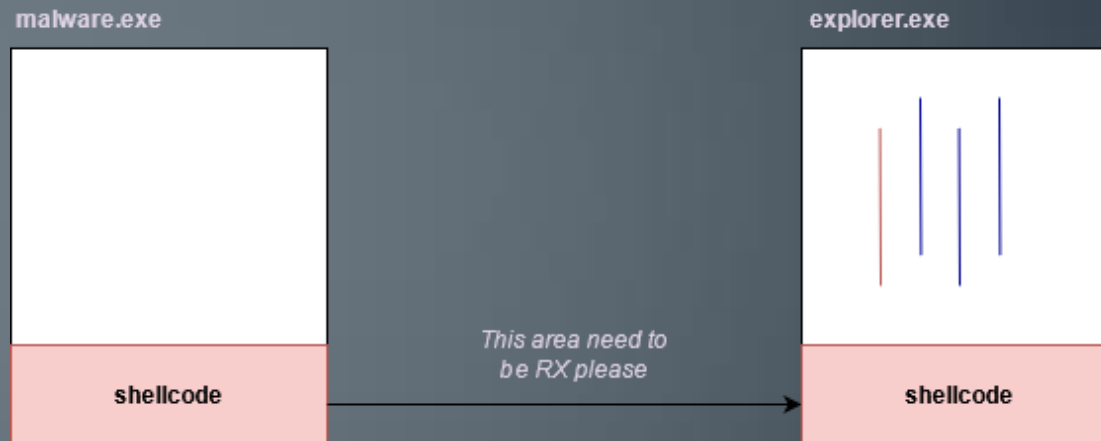
Thread Hijacking



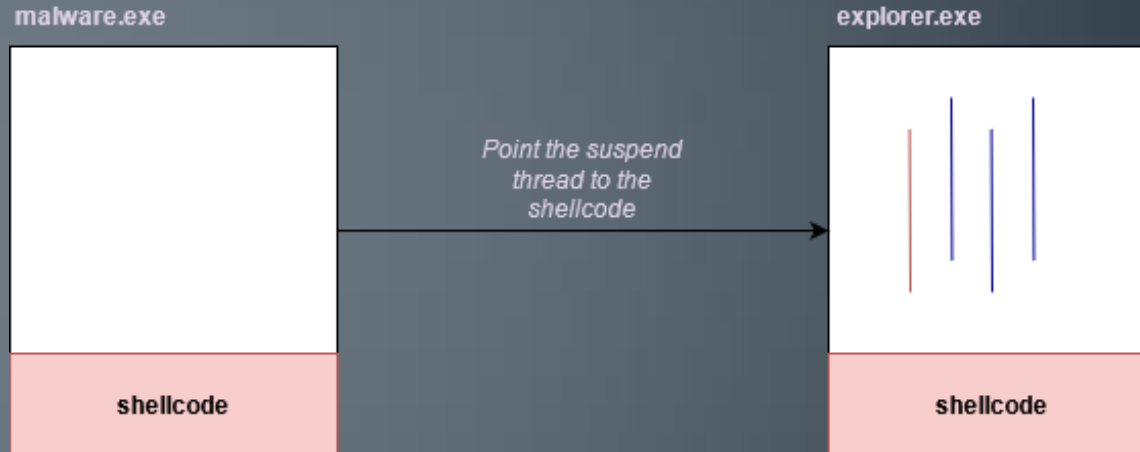
Thread Hijacking



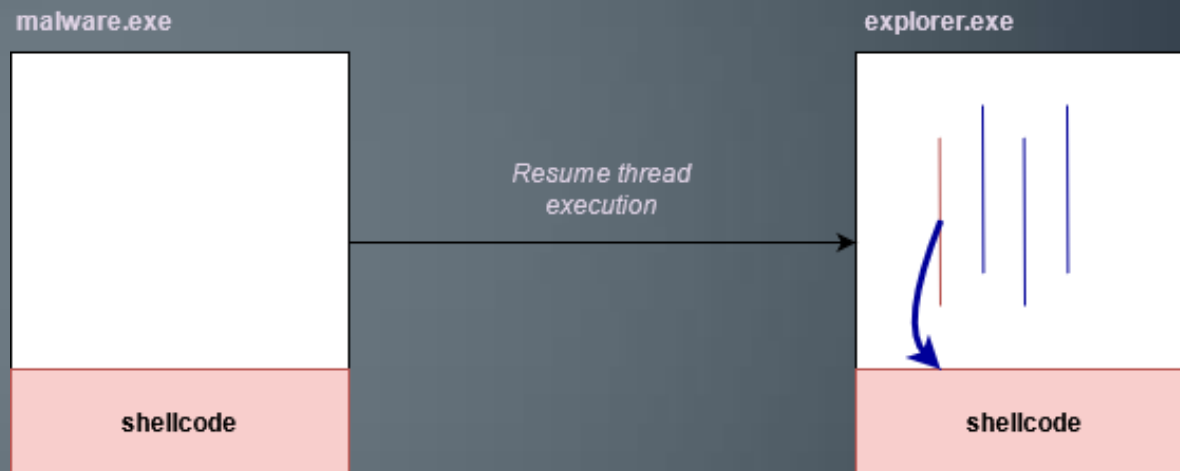
Thread Hijacking



Thread Hijacking



Thread Hijacking



The background of the slide features a series of thin, vertical, light blue lines of varying heights and positions, creating a textured, rain-like effect. A solid teal horizontal band spans the width of the slide, positioned in the lower half. The title text is centered within this band.

MapView Injection

Benefit(s)

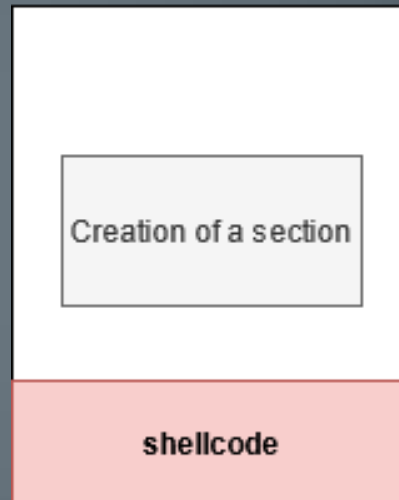
- No use of the Windows API « WriteProcessMemory » or « NtWriteVirtualMemory » (can be monitored by security product)

Common Windows API/function:

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

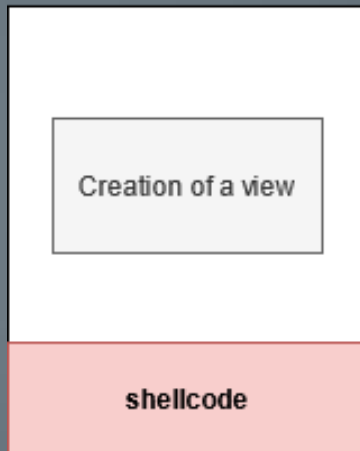
MapView Injection

malware.exe



MapView Injection

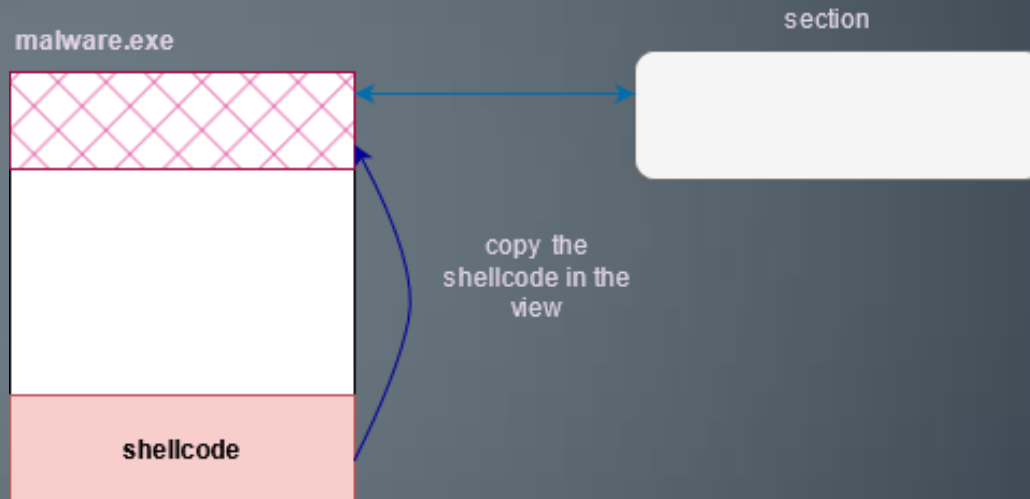
malware.exe



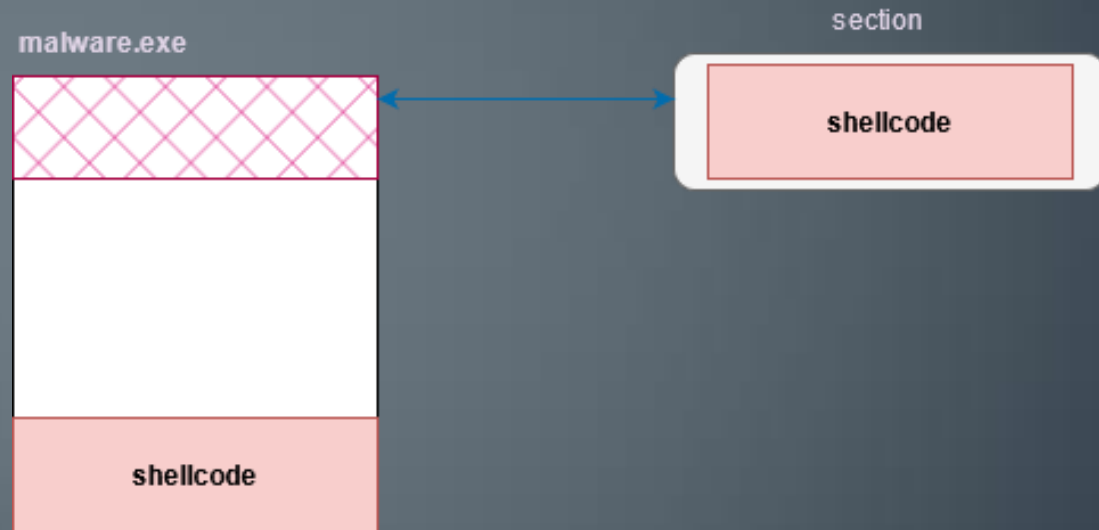
section



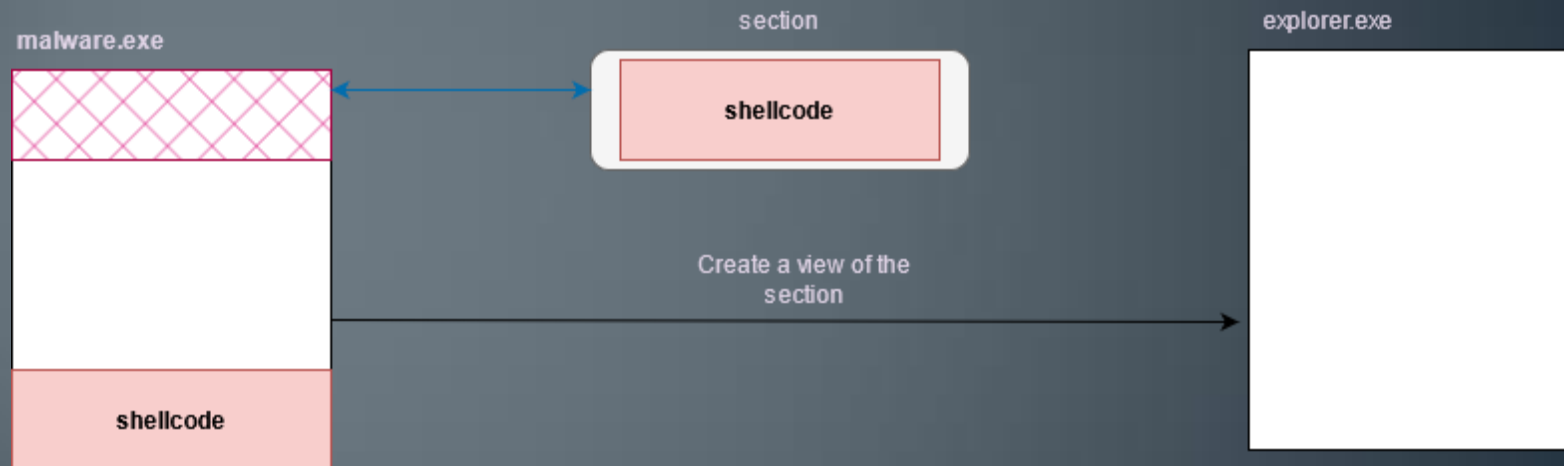
MapView Injection



MapView Injection



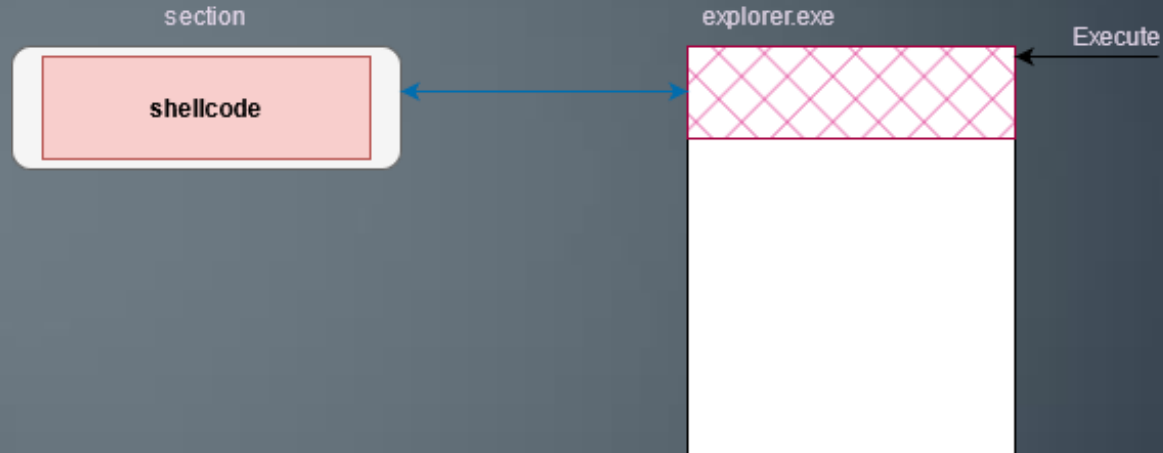
MapView Injection



MapView Injection



MapView Injection



The background of the slide features a series of thin, vertical, light blue lines of varying heights and positions, creating a textured, rain-like effect. A solid teal horizontal band spans the width of the slide, positioned in the lower half. The text 'Bonus: Hybrid Injection' is centered within this band.

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



PE-SIEVE

- <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!