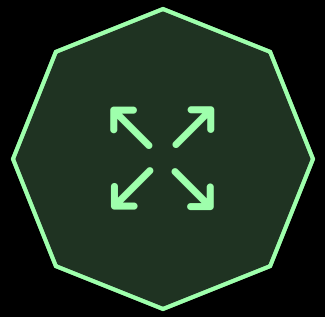
Unpacking Stubs

Types of Unpacking Stubs

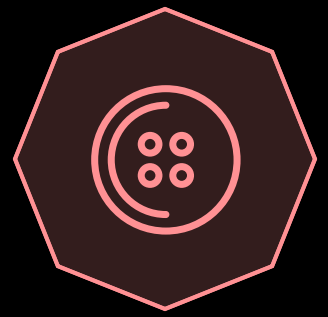


OWN PROCESS UNPACKING

- e.g. UPX, Wibu

PROCESS INJECTION UNPACKING

- e.g. Process Hollowing aka RunPE



HYBRID

- injected process unpacks data into own process

Unpacking Stub - Steps

E.g.

- create new process
- find another process
- create new section
- increase section size

Target data can be:

- PE EXE
- PE DLL
- shellcode
- section

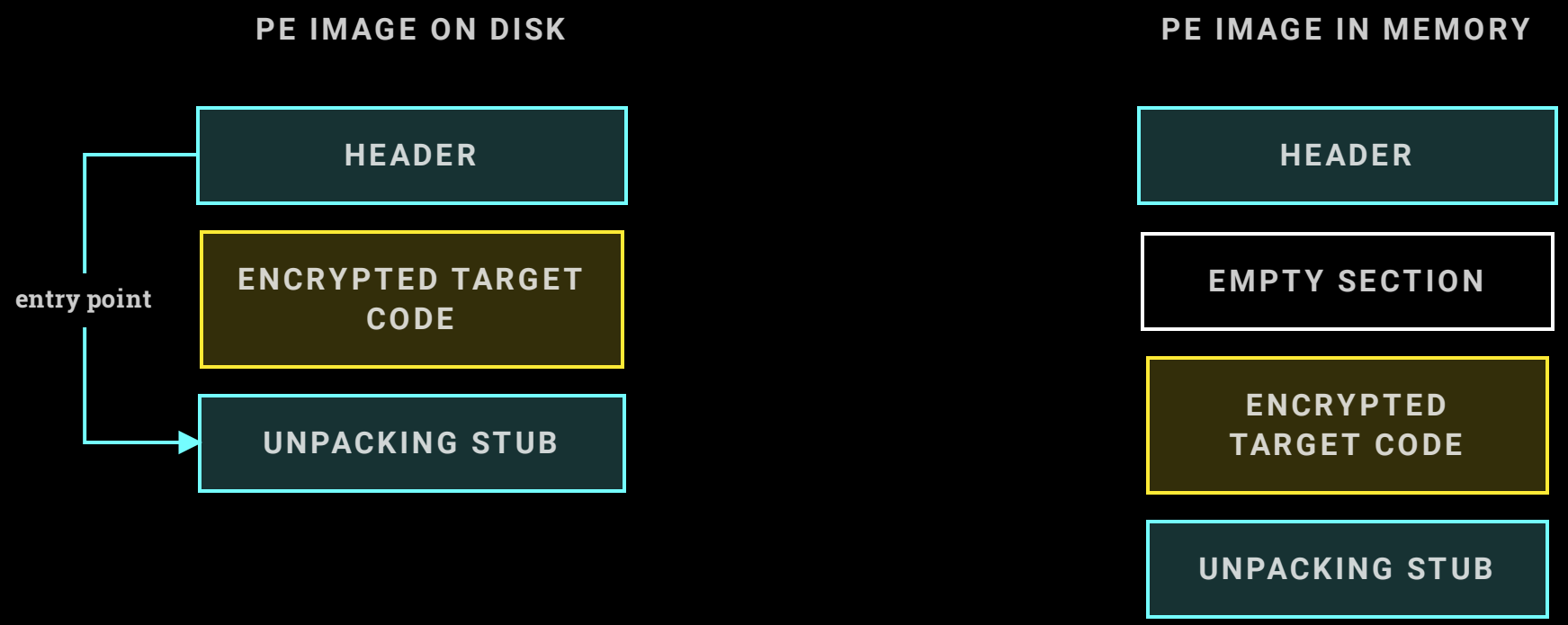
Execute target

Prepare target location, e.g.

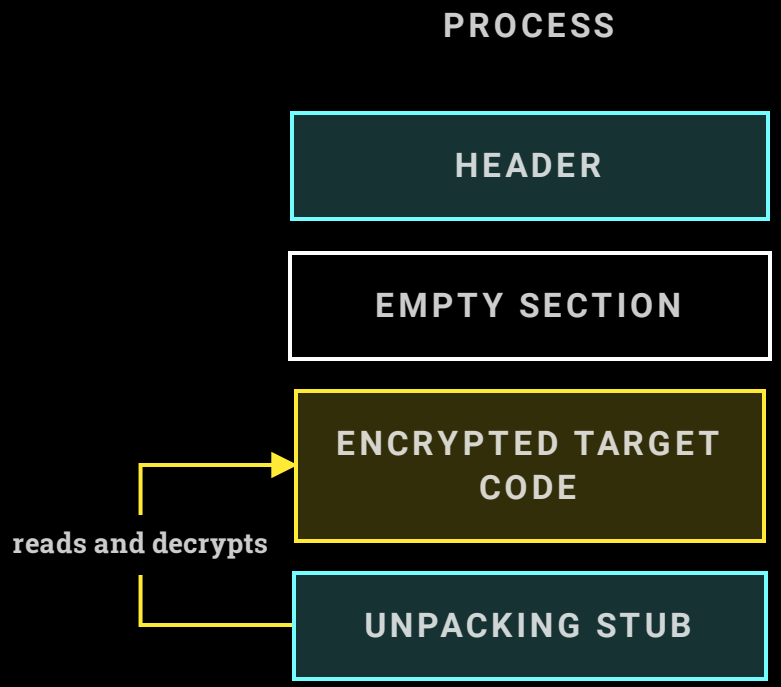
- carving the process
- adding RWX rights

- final preparation, e.g., set entry point in target

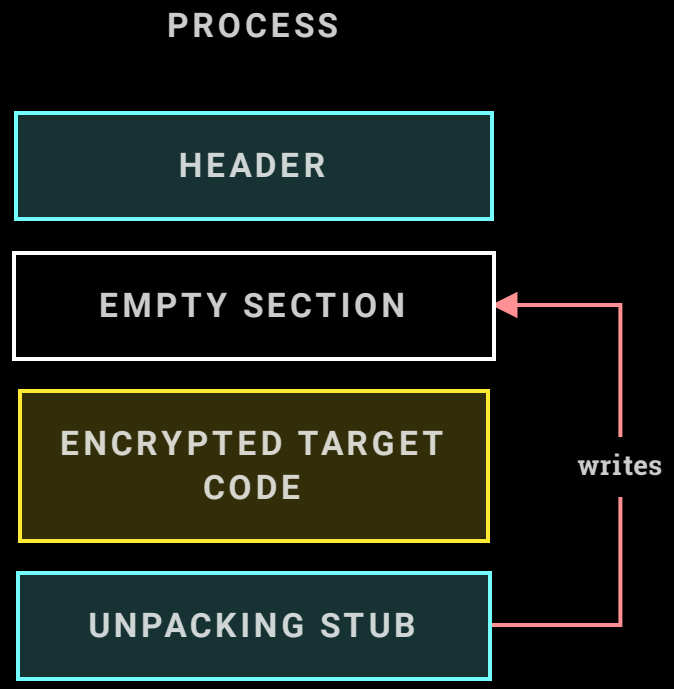
Own Process Execution - Virtual Section



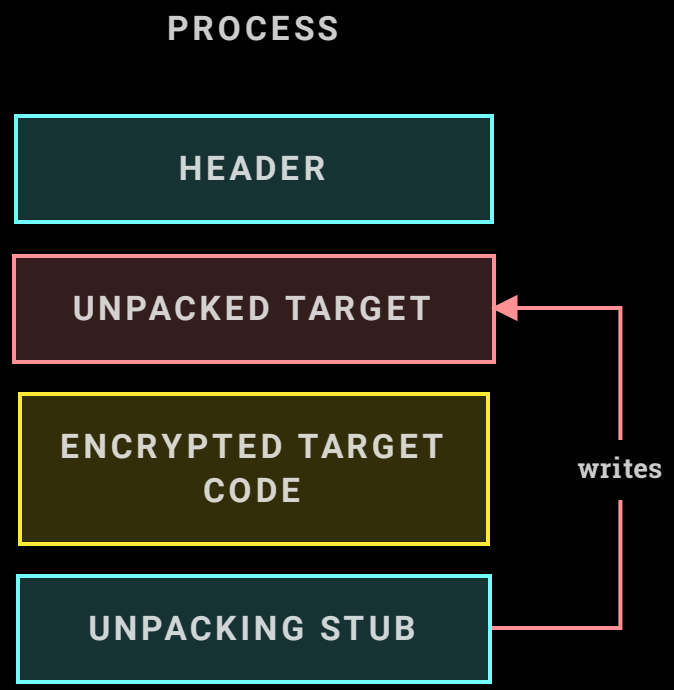
Own Process Execution - Virtual Section



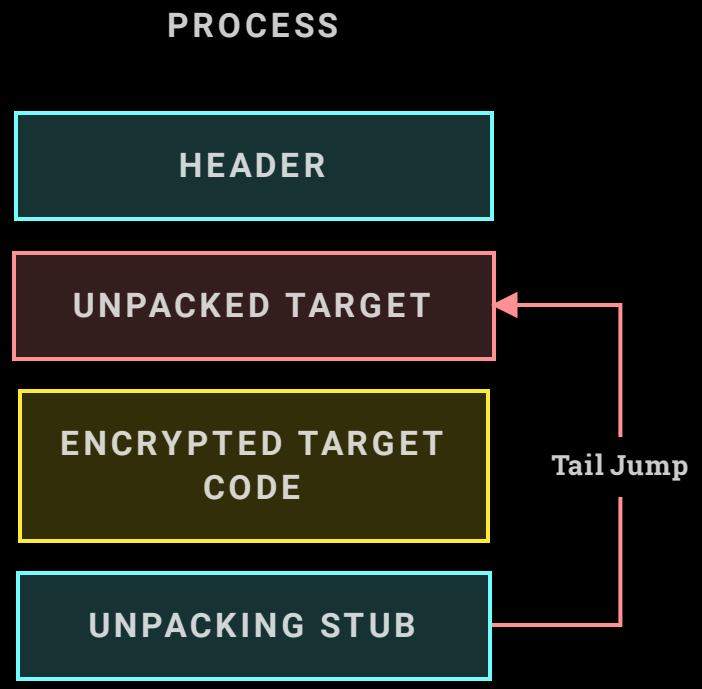
Own Process Execution - Virtual Section



Own Process Execution - Virtual Section



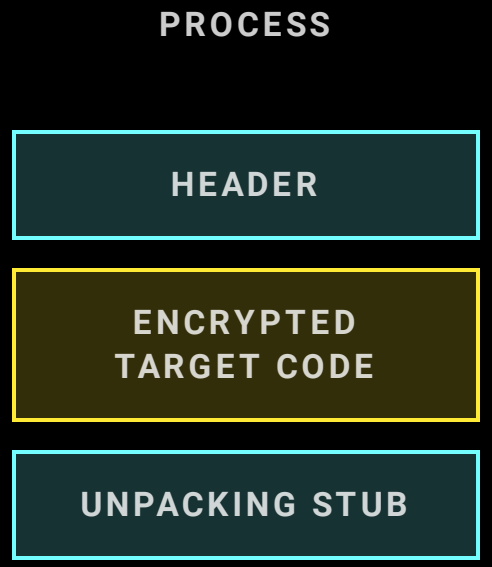
Own Process Execution - Virtual Section



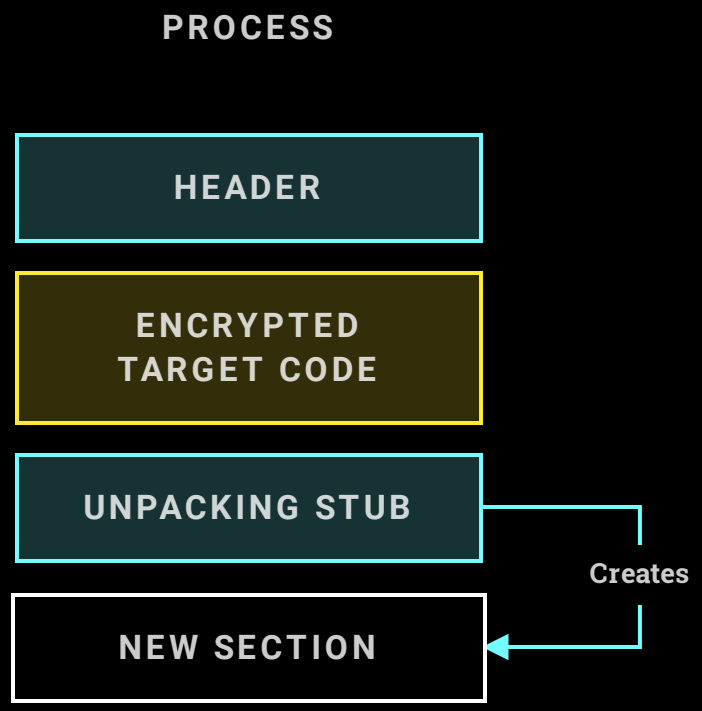
The tail jump is the jump to the original entry point (OEP)

The tail jump usually hops into a different section

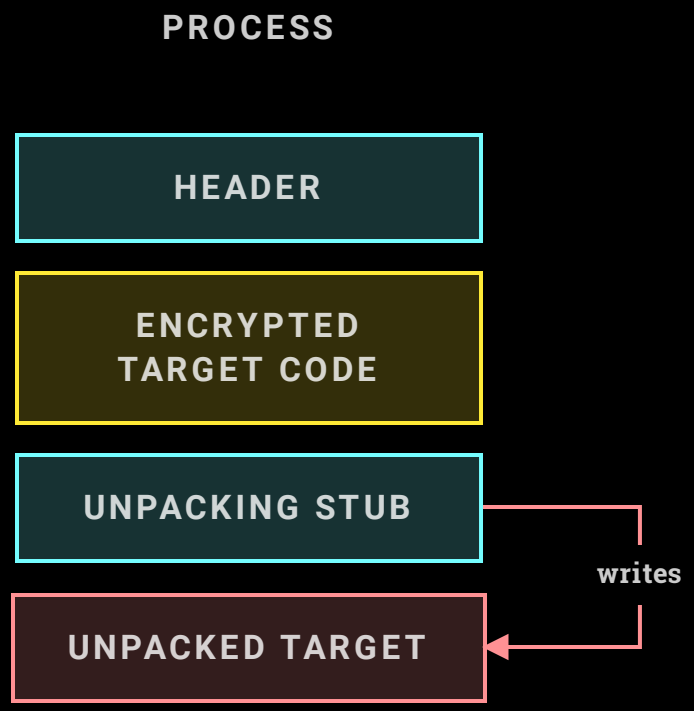
Own Process Execution - New Section



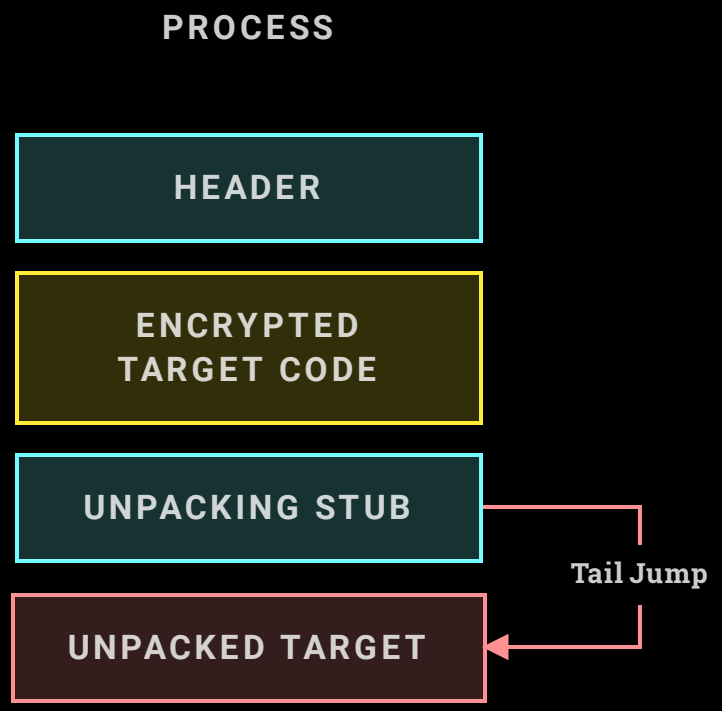
Own Process Execution - New Section



Own Process Execution - New Section



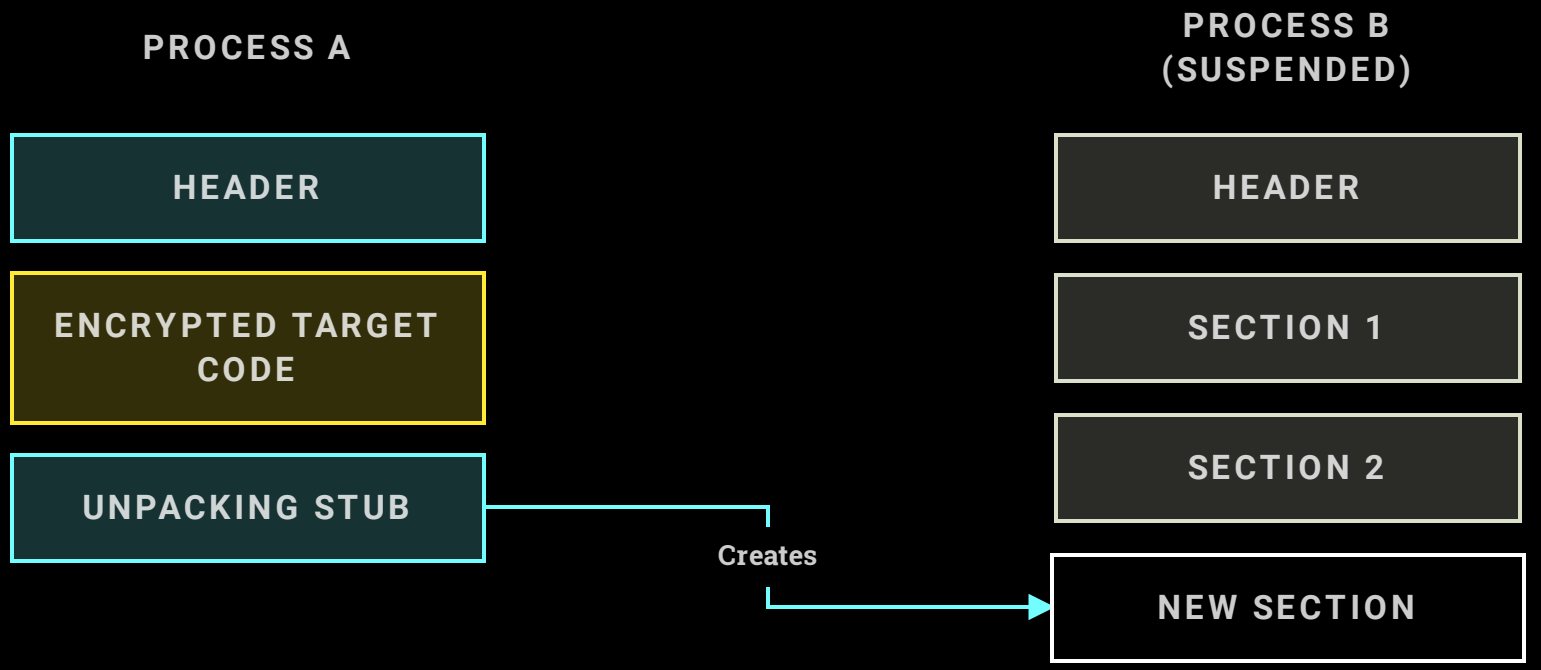
Own Process Execution - New Section



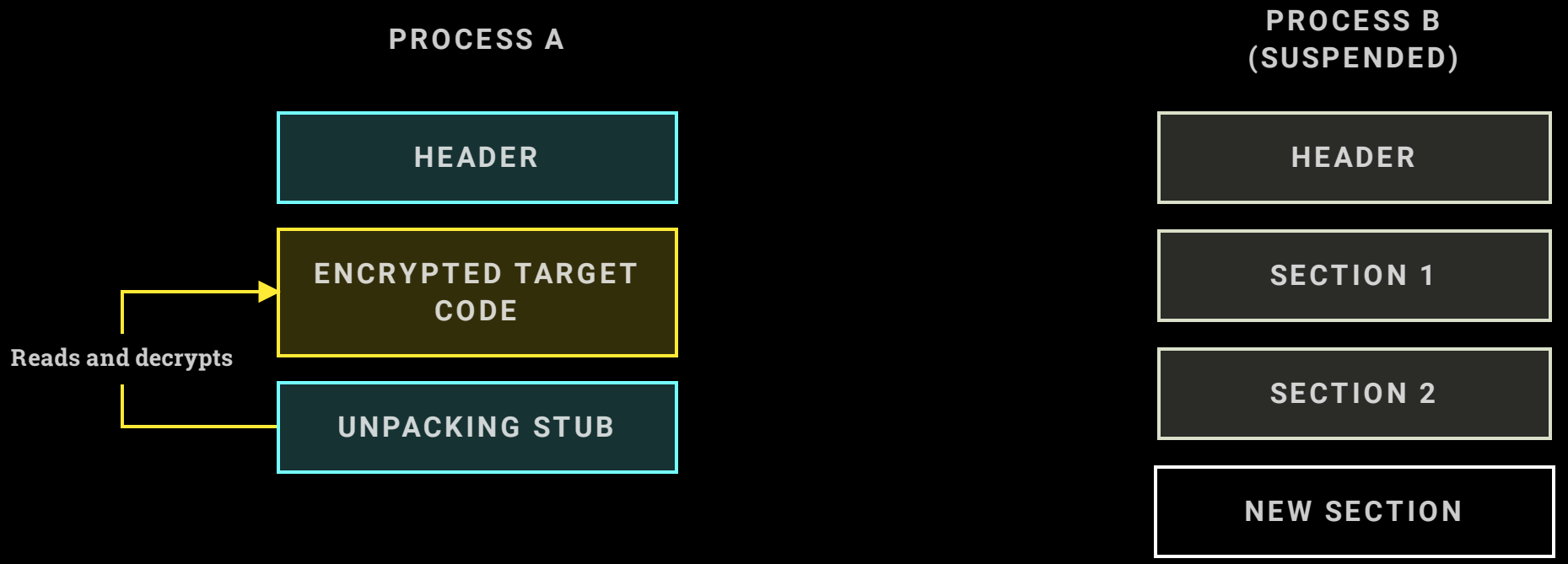
Process Injection Execution - New Section

Process Injection Execution - New Section

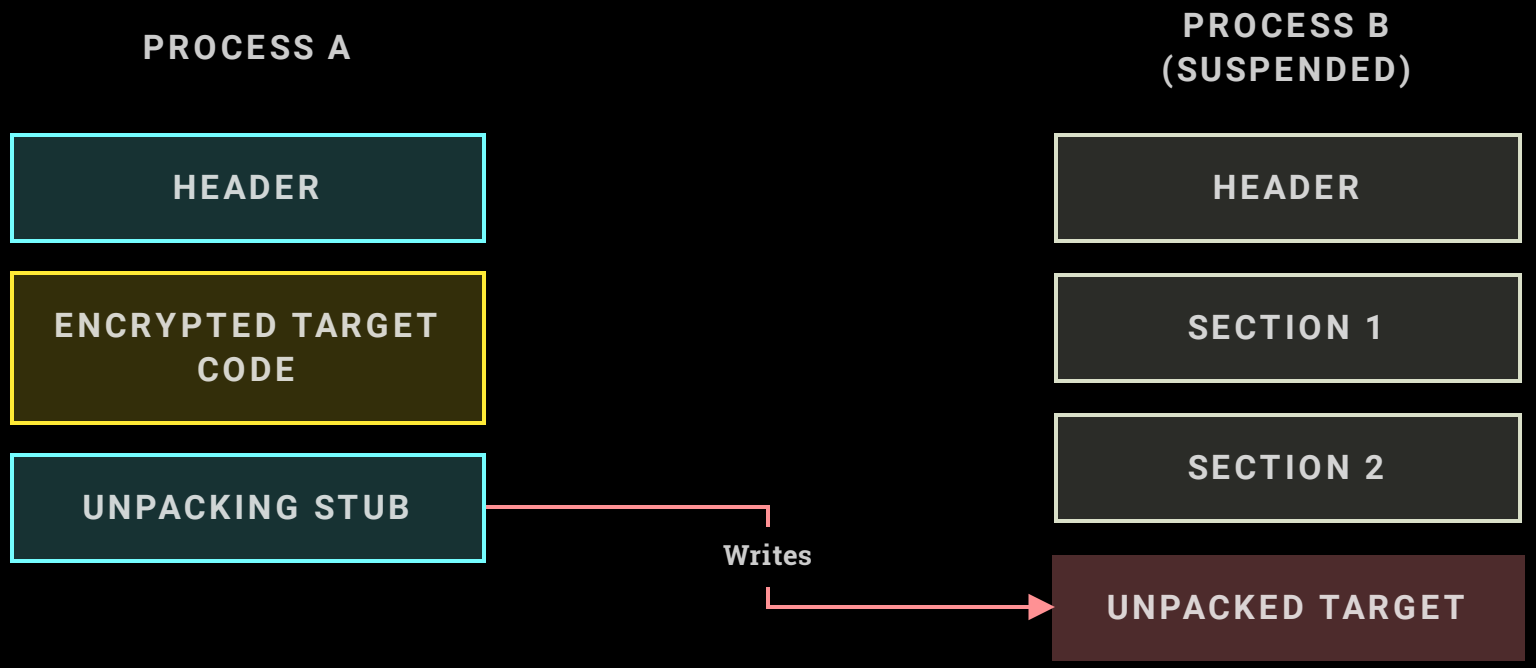
Process Injection Execution - New Section



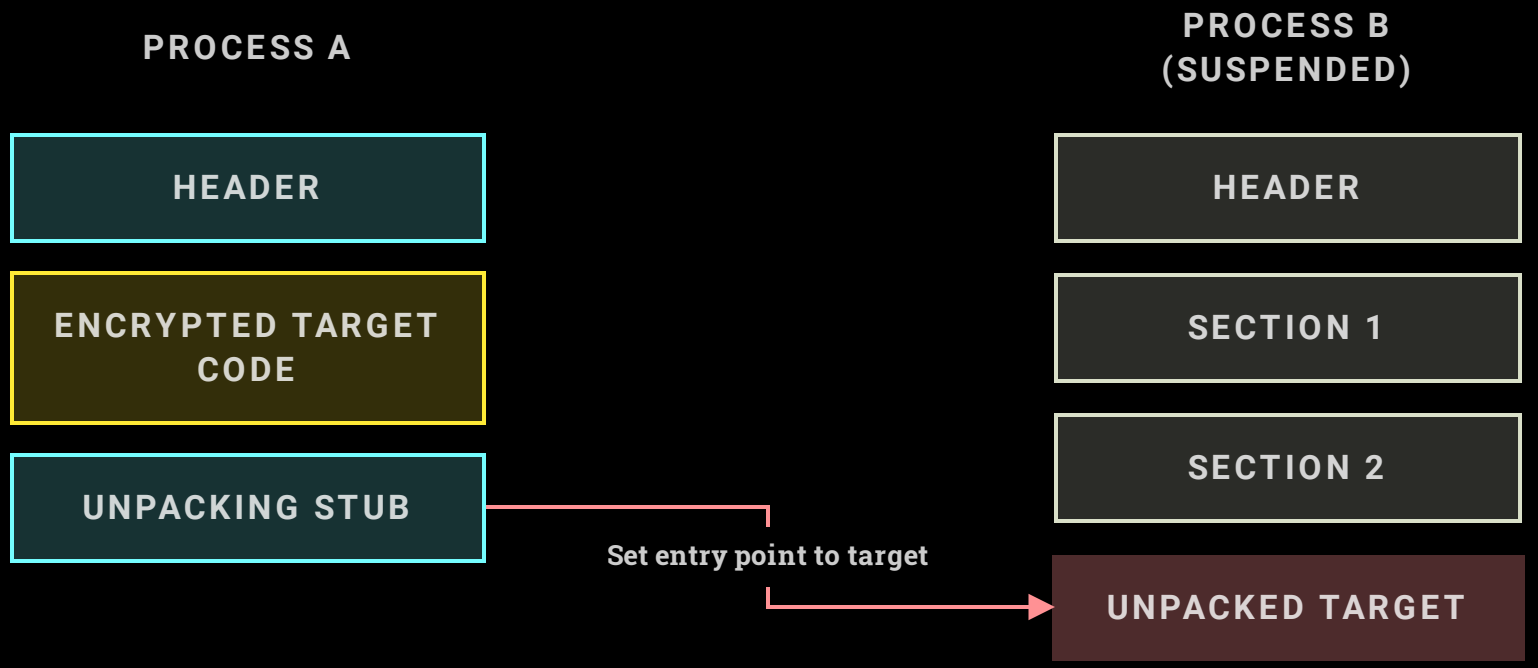
Process Injection Execution - New Section



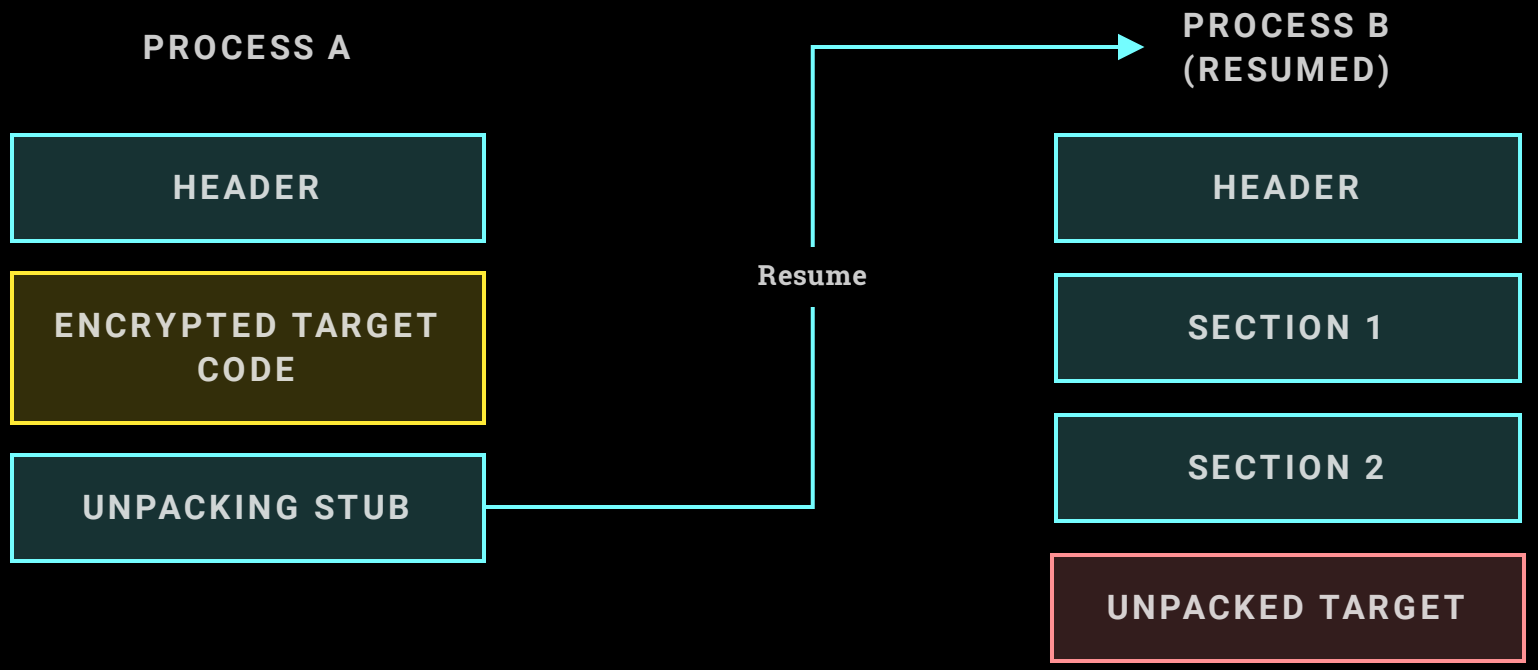
Process Injection Execution - New Section



Process Injection Execution - New Section

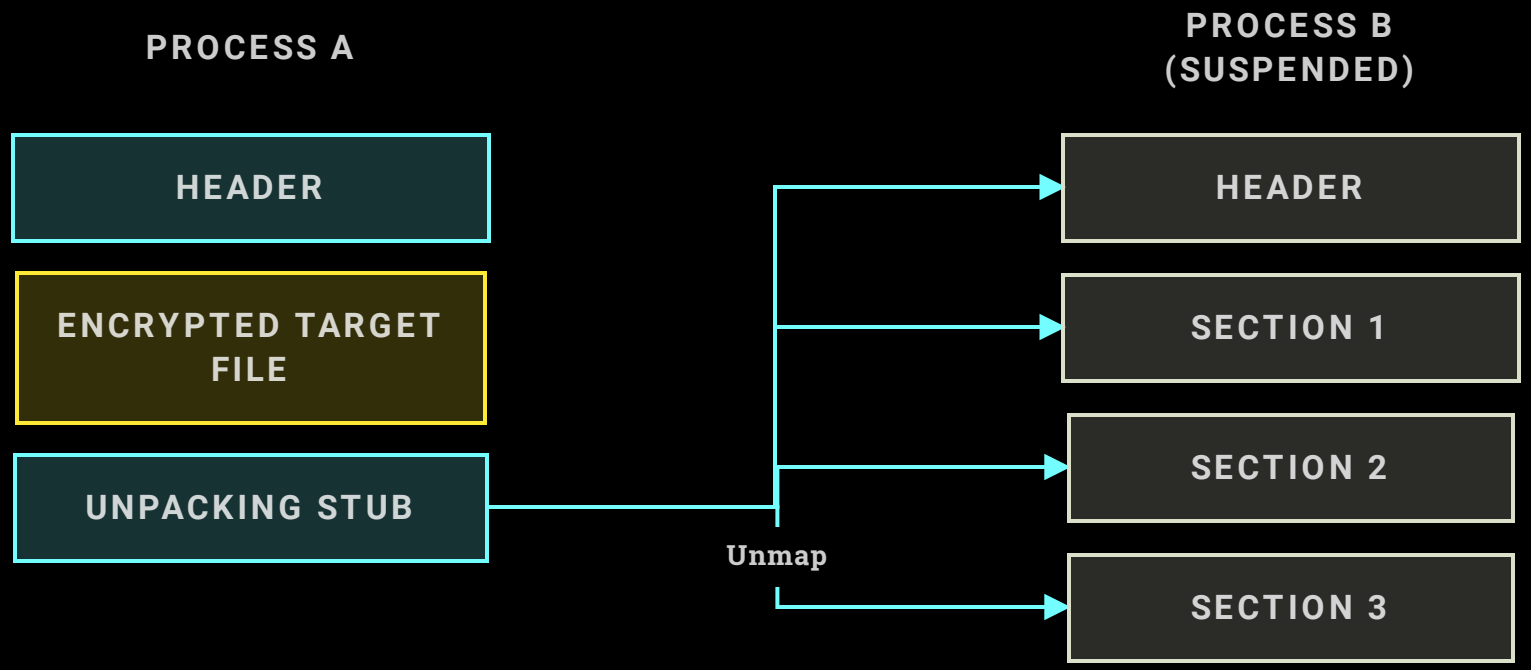


Process Injection Execution - New Section

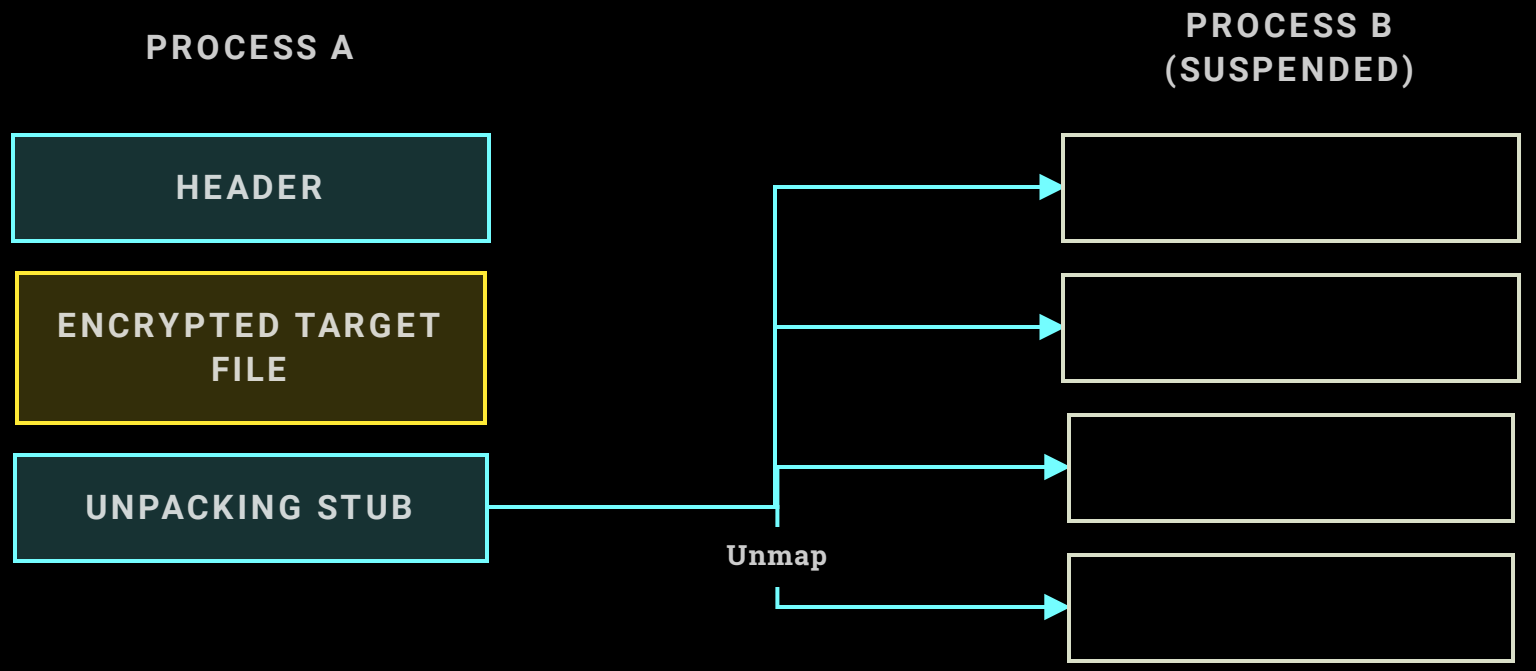


Process Injection Execution - RunPE

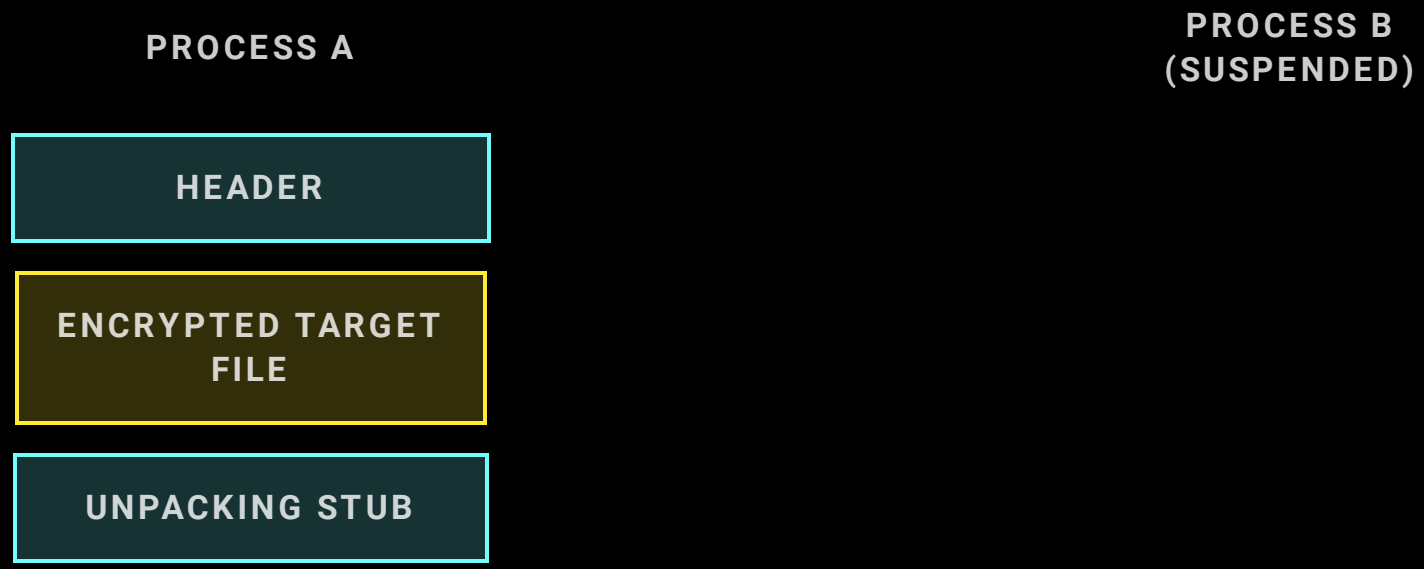
Process Injection Execution - RunPE



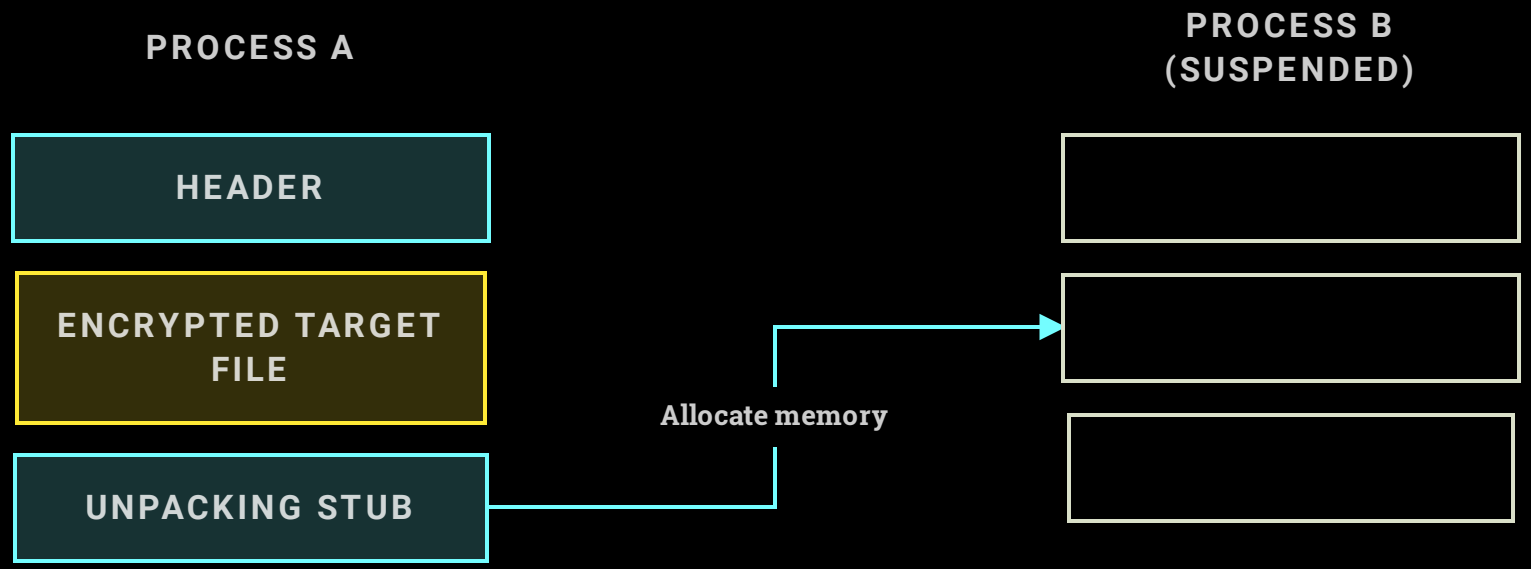
Process Injection Execution - RunPE



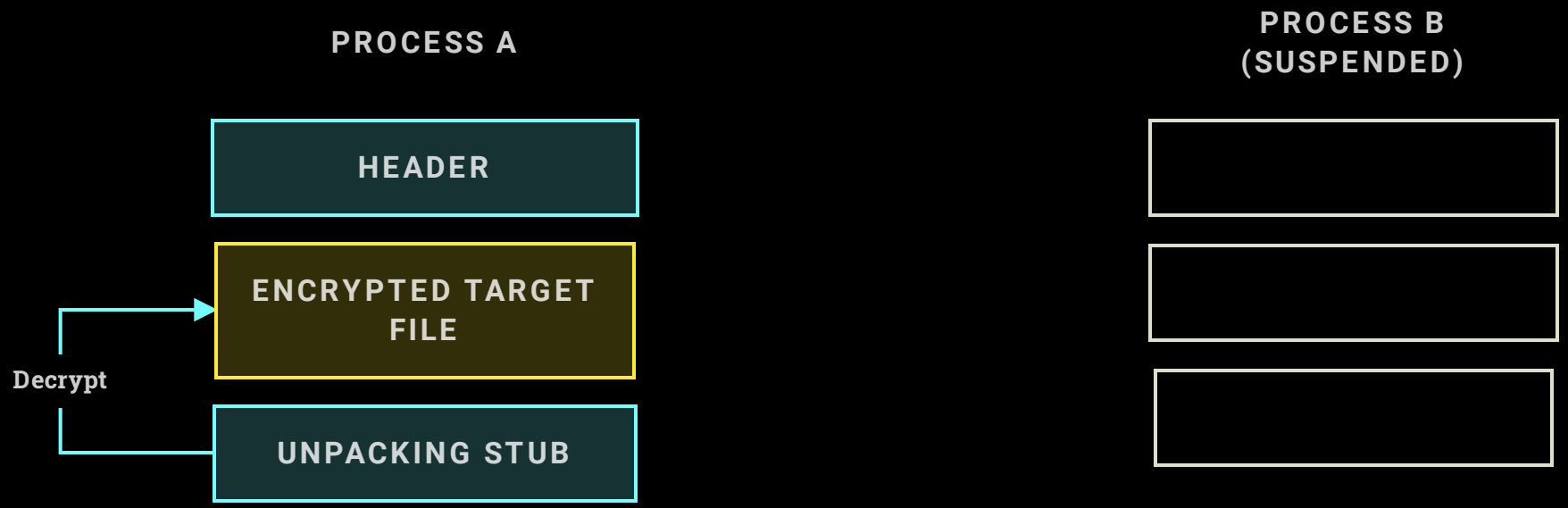
Process Injection Execution - RunPE



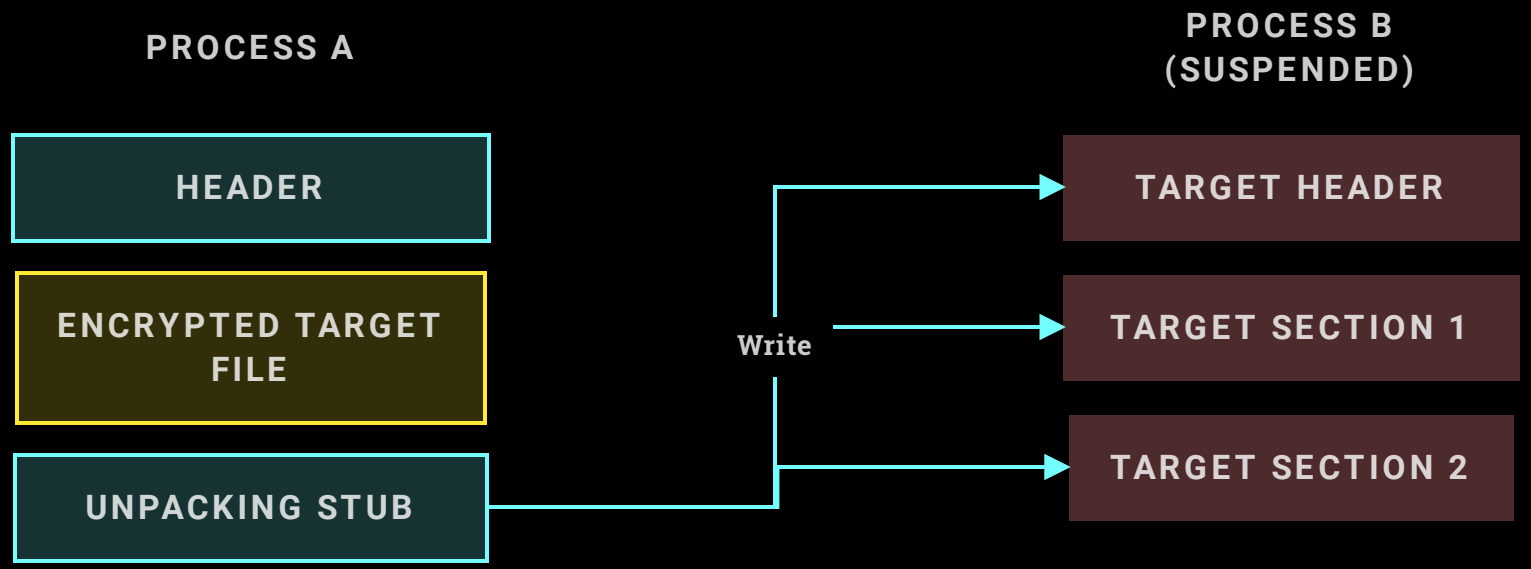
Process Injection Execution - RunPE



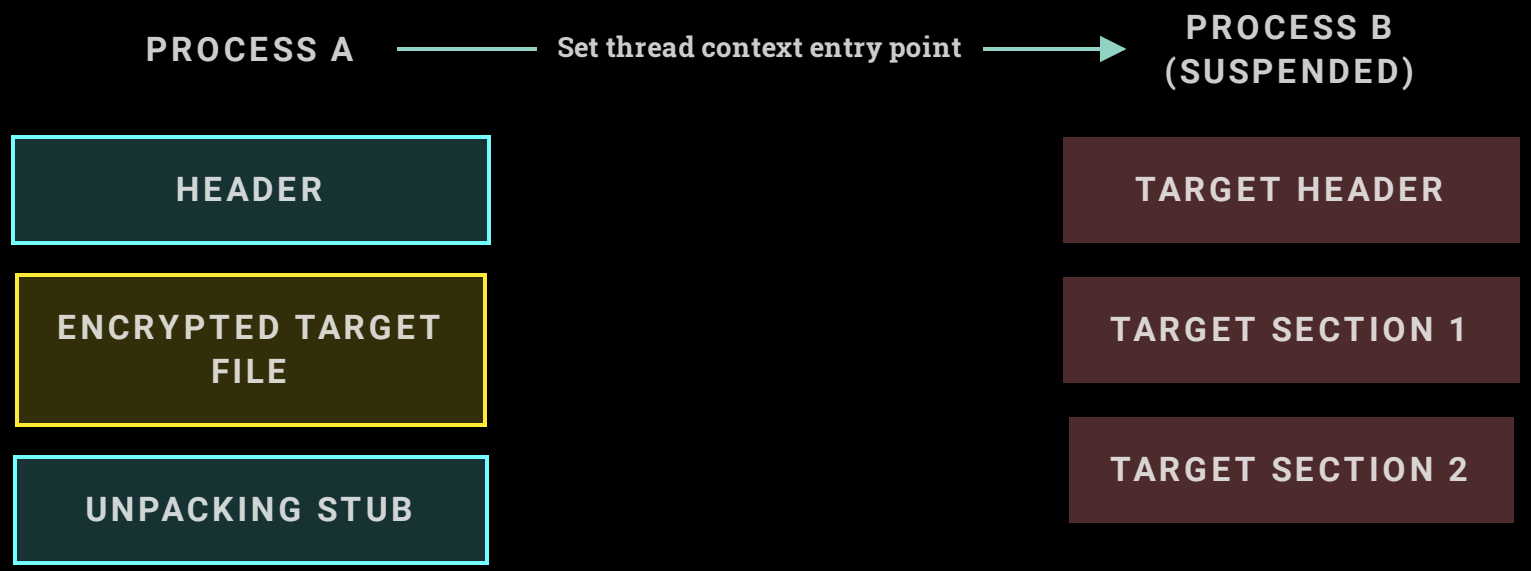
Process Injection Execution - RunPE



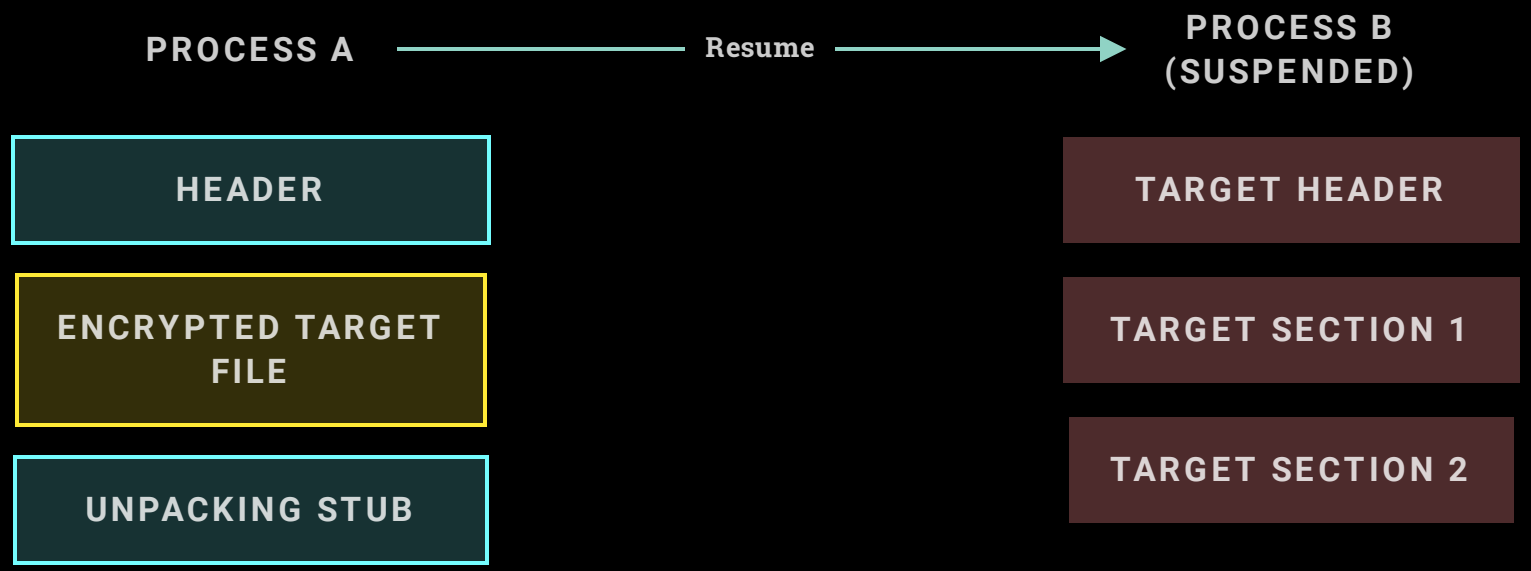
Process Injection Execution - RunPE



Process Injection Execution - RunPE



Process Injection Execution - RunPE



Process Injection Execution - RunPE