Self Injection

What is self injection

- **Self-Injection is a way to have most of the malware code encrypted, but later during the execution, the malware decrypts the malicious code in-memory and then transfer the execution to the newly unpacked malicious code.**
- Commonly used in packers (malware packer is **a tool used to mask a malicious file**)
- Overwrites the original executable with the actual payload
- Unpacking code will **decrypt the shellcode responsible for decrypting payload and overwriting**
- Simple to detect and locate a payload while debugging