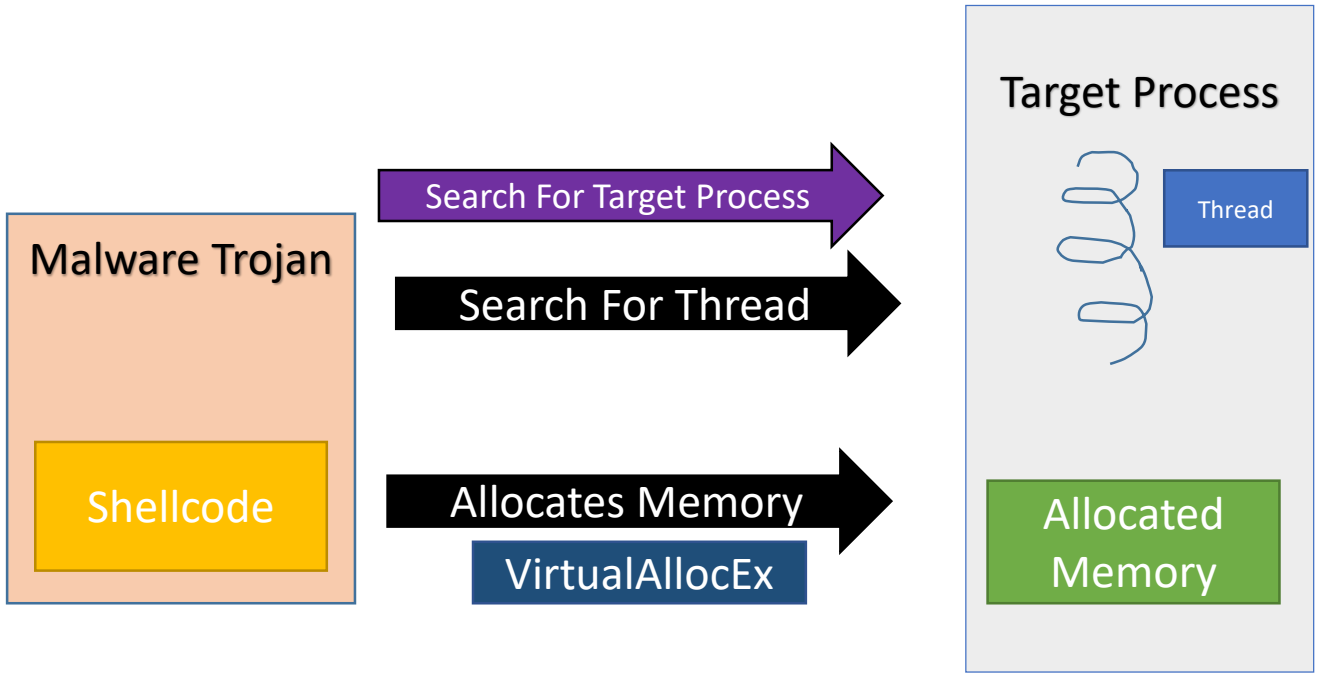
Thread Context Injection

Injecting Payload To Another Thread

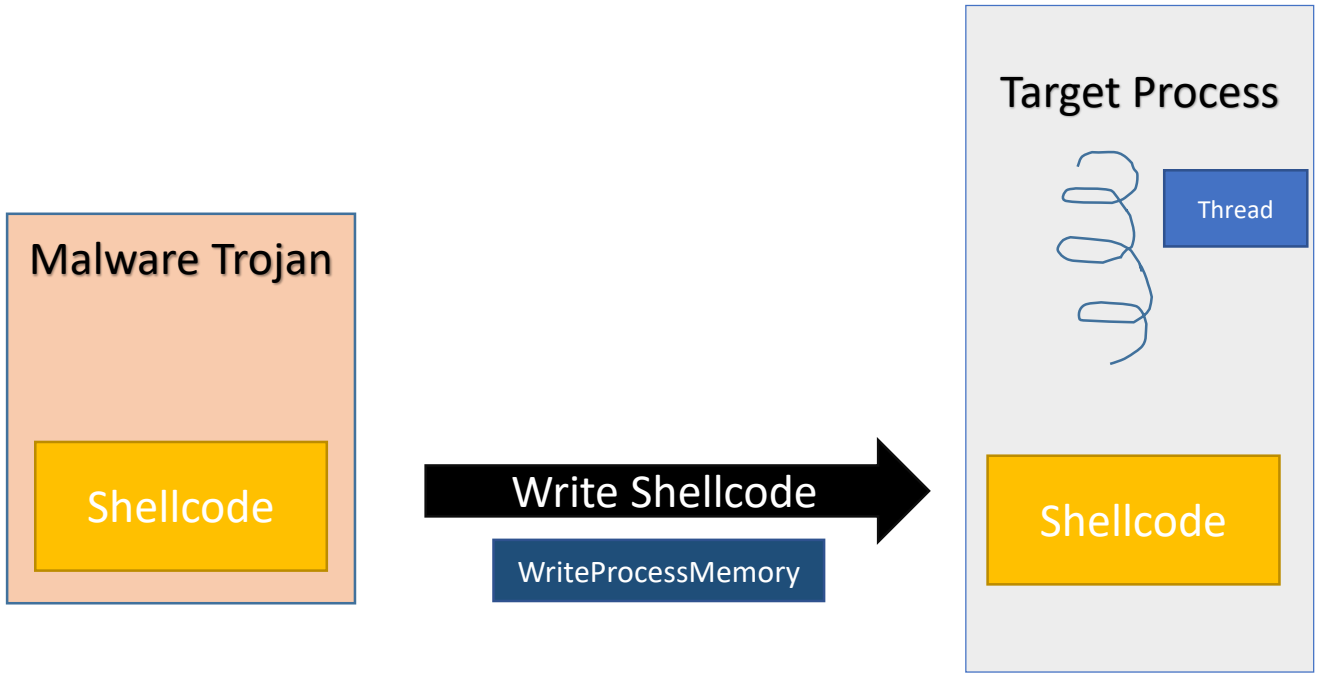
What is Thread Context?

- Information about a thread
- Memory allocation
- Heap, Stack
- Register values
- Next Instruction Pointer

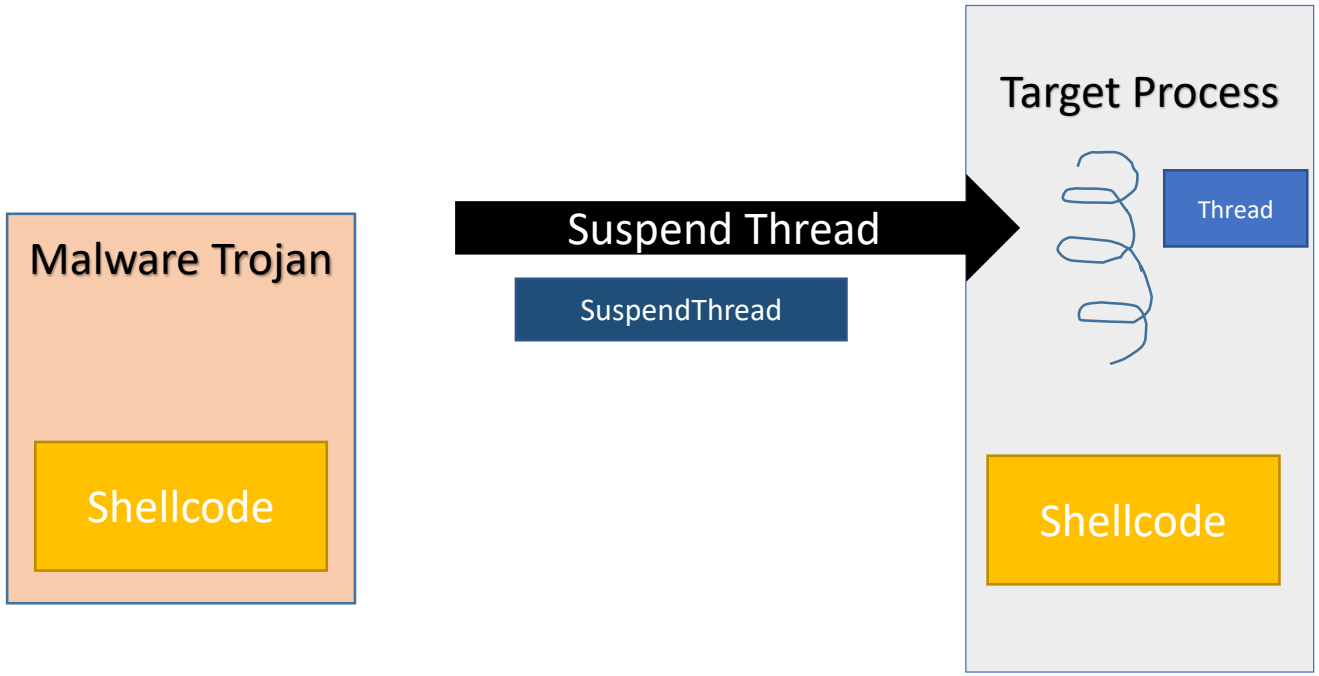
Mechanism of Thread Context Injection



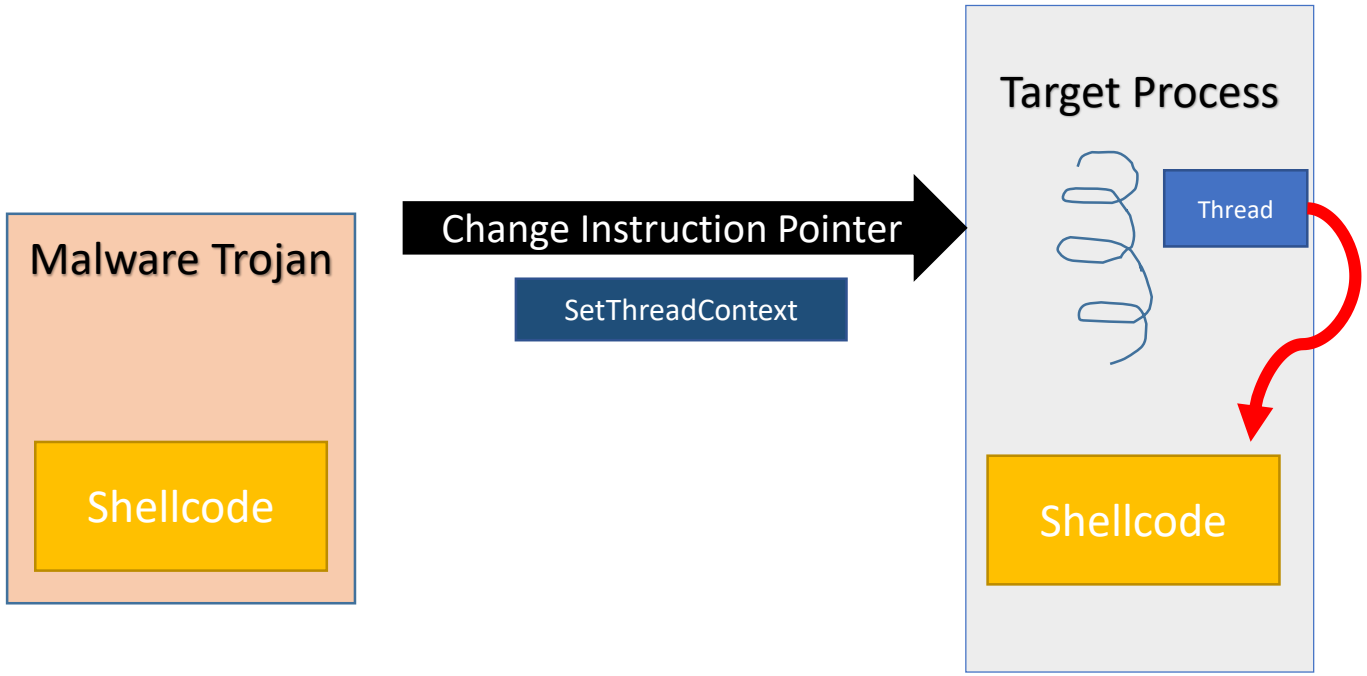
Mechanism of Thread Context Injection



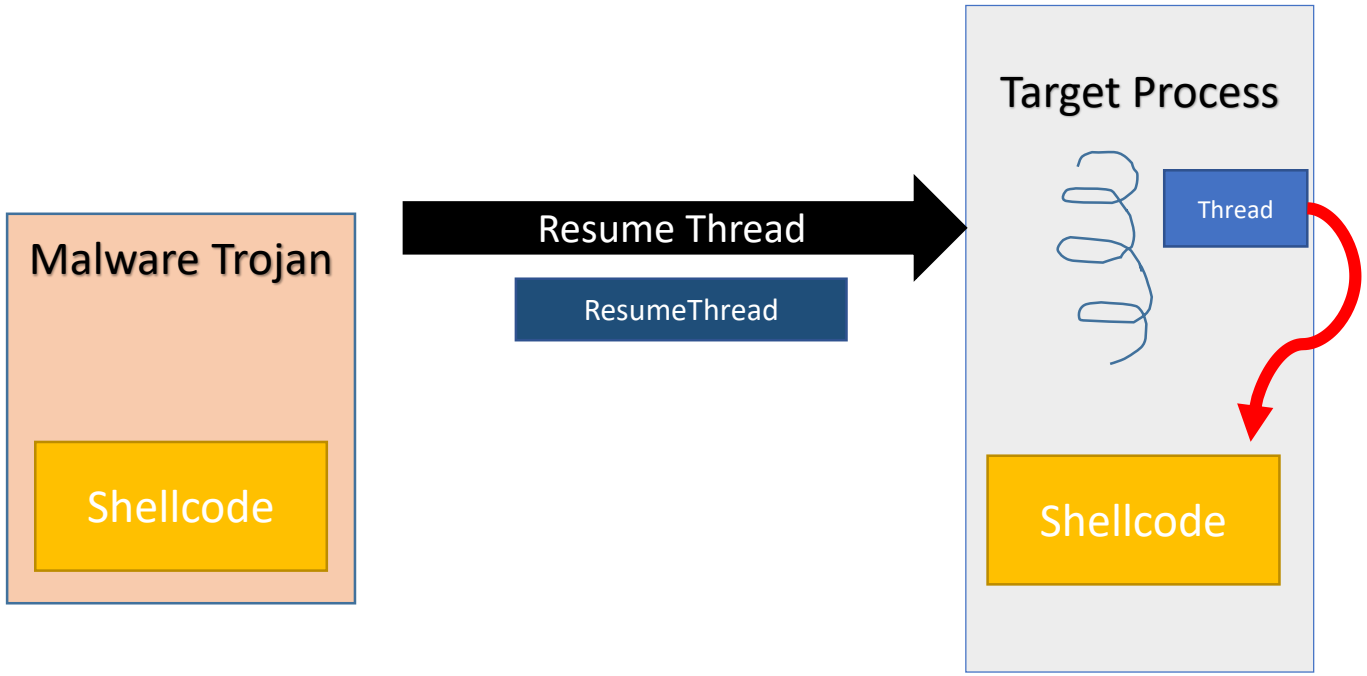
Mechanism of Thread Context Injection



Mechanism of Thread Context Injection



Mechanism of Thread Context Injection



Advantages & Disadvantages

Of Thread Context Injection

Advantages

- No need to Create Remote Thread
- Can use existing Thread
- More Stealthy

Disadvantages

- May crash the parent process of the thread, when the hijacked thread exits
- May disrupt what the original thread was doing
- It takes longer to inject

Thank you