Asynchronous Procedure Call Injection

Injecting Callback Functions on remote processes

Basic Concepts

- It is a kind of call-back function mechanism
- By putting instructions in memory queue of a running thread
- When the thread enters certain state, it will notice the queue and execute the instructions in the queue
- The term Asynchronous means not executing immediately, it can execute anytime in future.

Example of APC

- For example, if a process wants to read a file, it will make a request to the OS.
- But opening a file is slow, so the process will not stop and wait but allow the OS to open the file, while the process continues to do other things.
- Once the file is ready, the OS will inform the process.

Mechanism of APC Injection

1. Search for Thread

2. Allocate Memory

VirtualAllocEx

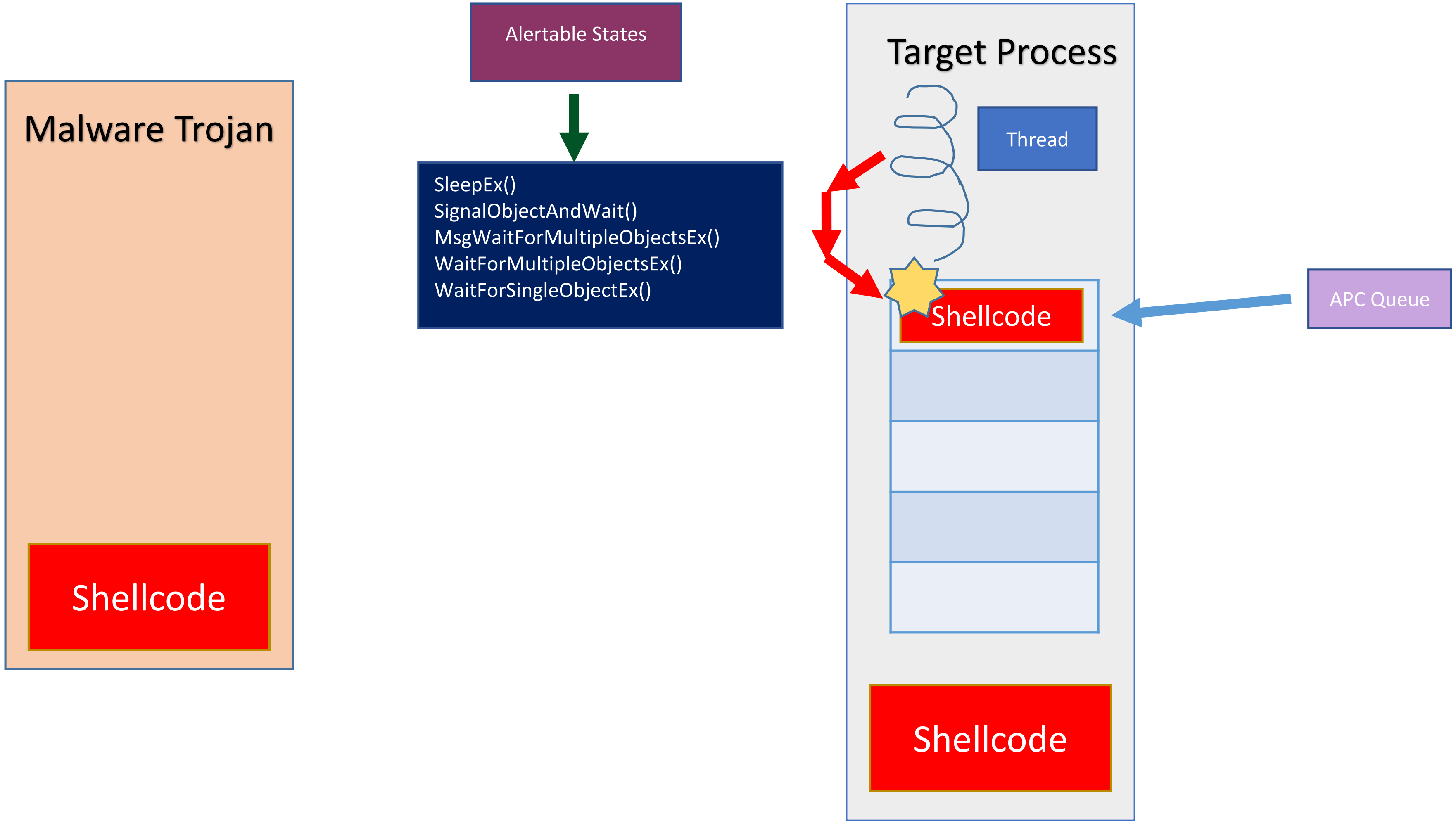
3. Copy Shellcode to Memory

WriteProcessMemory

4. Add job to Queue

QueueUserAPC

5. Wait for Thread to enter Alertable State



Malware Trojan

Shellcode

Alertable States

SleepEx()
SignalObjectAndWait()
MsgWaitForMultipleObjectsEx()
WaitForMultipleObjectsEx()
WaitForSingleObjectEx()

Target Process

Thread

Shellcode

APC Queue

Shellcode

Advantages & Disadvantages

Of Asynchronous Procedure Call Injection

Advantages

- Delayed execution of shellcode throws off causation between Malware and Target.
- Alertable State is triggered not by Malware but by Target Process, user will not suspect that the Malware Process is responsible

Disadvantages

- It needs to wait for Thread to enter Alertable State
- And is therefore slow and uncertain
- Uses VirtualAllocEx and WriteProcessMemory, which are usually detected by AV unless obfuscated

Thank you