Early Bird APC Injection

Achieving Camouflage by Hijacking a Legitimate Process before It hits Entry Point

Basic Concepts

- A malware creates a legitimate process in a suspended state
- Then, injects shellcode into it
- And inserts a job into the threads APC Queue
- And finally resumes the thread
- The shellcode executes before the process begins, to avoid detection by Anti-malware hooks

Mechanism of Early Bird APC Injection

1. Creates a Process in a Suspended State

2. Allocate Memory

VirtualAllocEx

3. Copy Shellcode to Memory

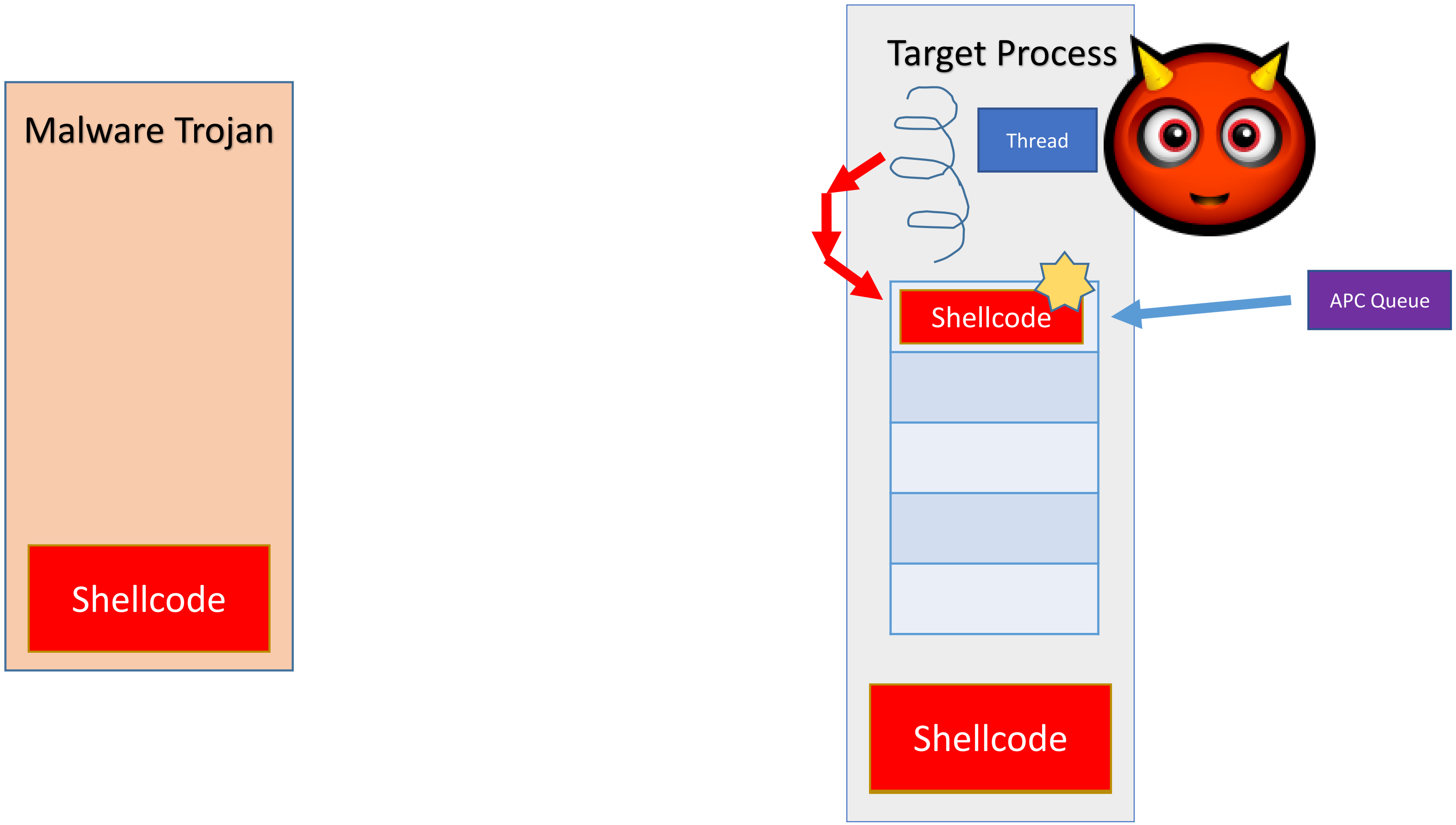
WriteProcessMemory

4. Add job to Queue

QueueUserAPC

5. Resumes Thread

ResumeThread



Advantages & Disadvantages

Of Early Bird APC Injection

Advantages

- Camouflages the execution of the malicious shellcode by hijacking a legitimate process before it hits entry point
- The remaining code of the actual legitimate process is abandoned whilst the shellcode runs
- Bypasses security product hooks.
- The shellcode executes before the process begins to avoid detection by Anti-malware hooks
- Runs with application icon of the original process.

Disadvantages

- Uses VirtualAllocEx and WriteProcessMemory, which are usually detected by AV unless obfuscated
- May occasionally crash upon exit

Thank you