APC INJECTION

What is APC Injection

> APC = Asynchronous Procedure Call

- APC injection is a method of executing arbitrary code in the address space of a separate live process.
- Allows Malware to target already running threads to execute malicious code.

Process of APC Injection

- When threads are placed in a **alertable state** through calls such as `SleepEx` , queued APCs are executed.
- A handle to an existing victim process is first created with native Windows API calls such as `OpenThread`. At this point `QueueUserAPC` can be used to invoke a function (such as `LoadLibrayA` pointing to a malicious DLL).
- As a result malware can call it's own APCs to achieve injection without calling **AV-Recognizable** API calls.

> Windows API calls such as `SuspendThread`/`SetThreadContext`/`ResumeThread`, `QueueUserAPC`/`NtQueueApcThread`, and those that can be used to modify memory within another process, such as `VirtualAllocEx`/`WriteProcessMemory`, may be used for this technique

```
if (Thread32First(snapshot, &threadEntry)) {
    do {
        if (threadEntry.th32OwnerProcessID == processEntry.th32ProcessID) {
            threadIds.push_back(threadEntry.th32ThreadID);
        }
    } while (Thread32Next(snapshot, &threadEntry));
}

for (DWORD threadId : threadIds) {
    threadHandle = OpenThread(THREAD_ALL_ACCESS, TRUE, threadId);
    QueueUserAPC((PAPCFUNC)apcRoutine, threadHandle, NULL);
    Sleep(1000 * 2);
}
```