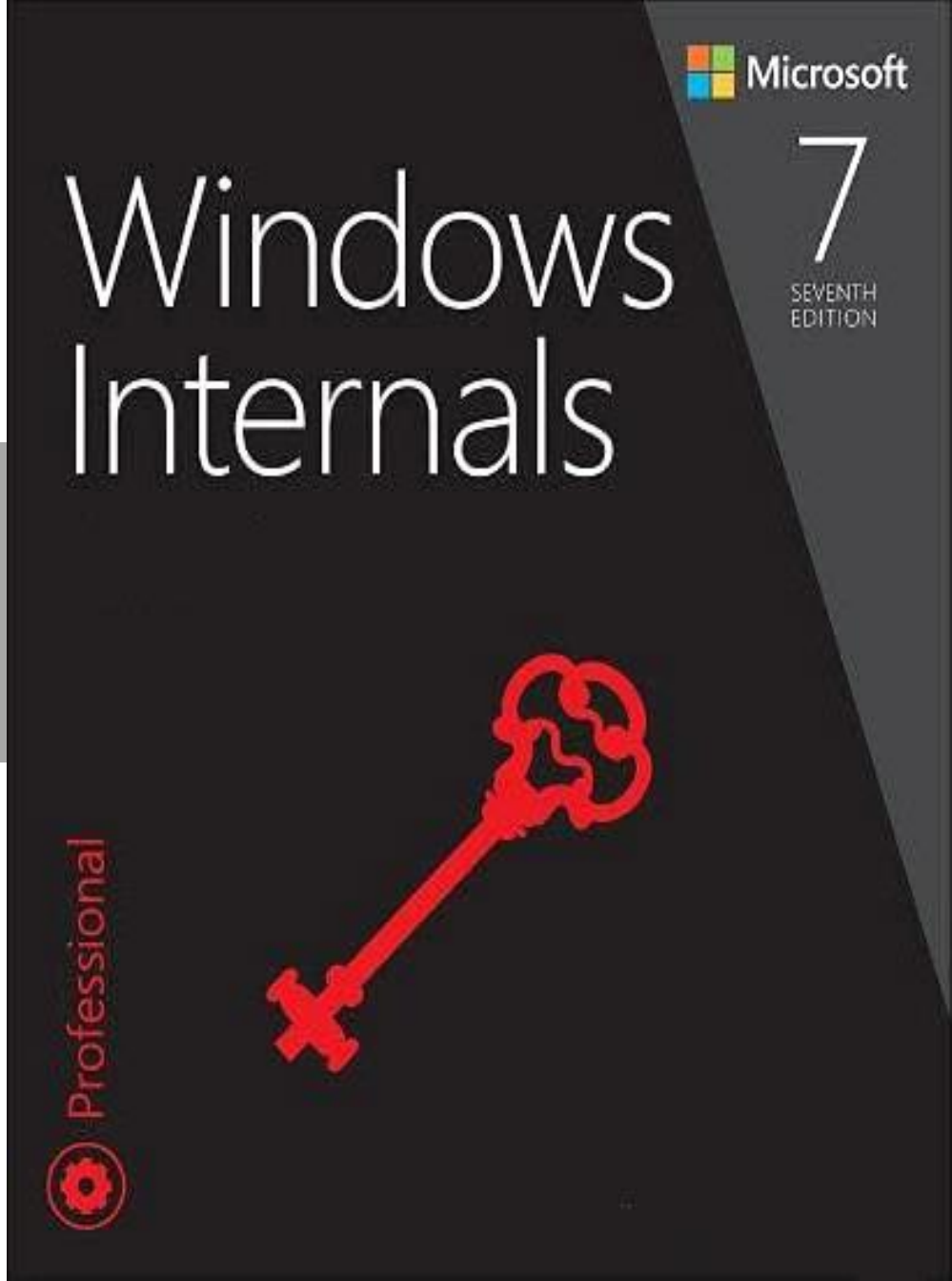
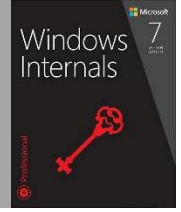
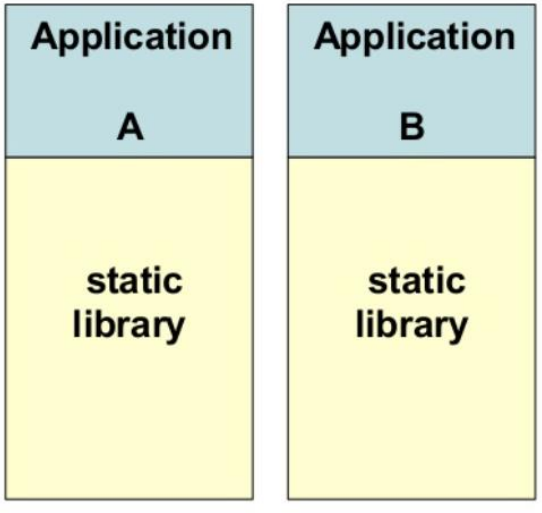
01) Threads
Remote Threads



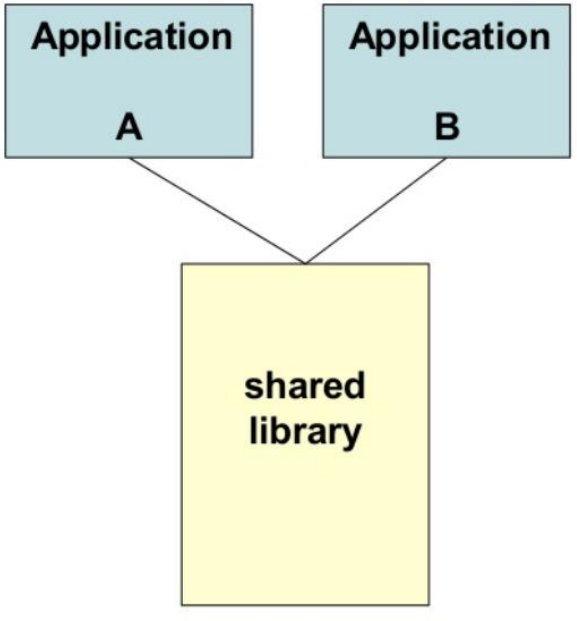
DLL (Dynamic Link Library)?



Static Library vs. Shared Library



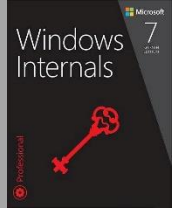
Static library



Shared library

achindrabhatnagar.wordpress.com

Creating a Thread in Another Process

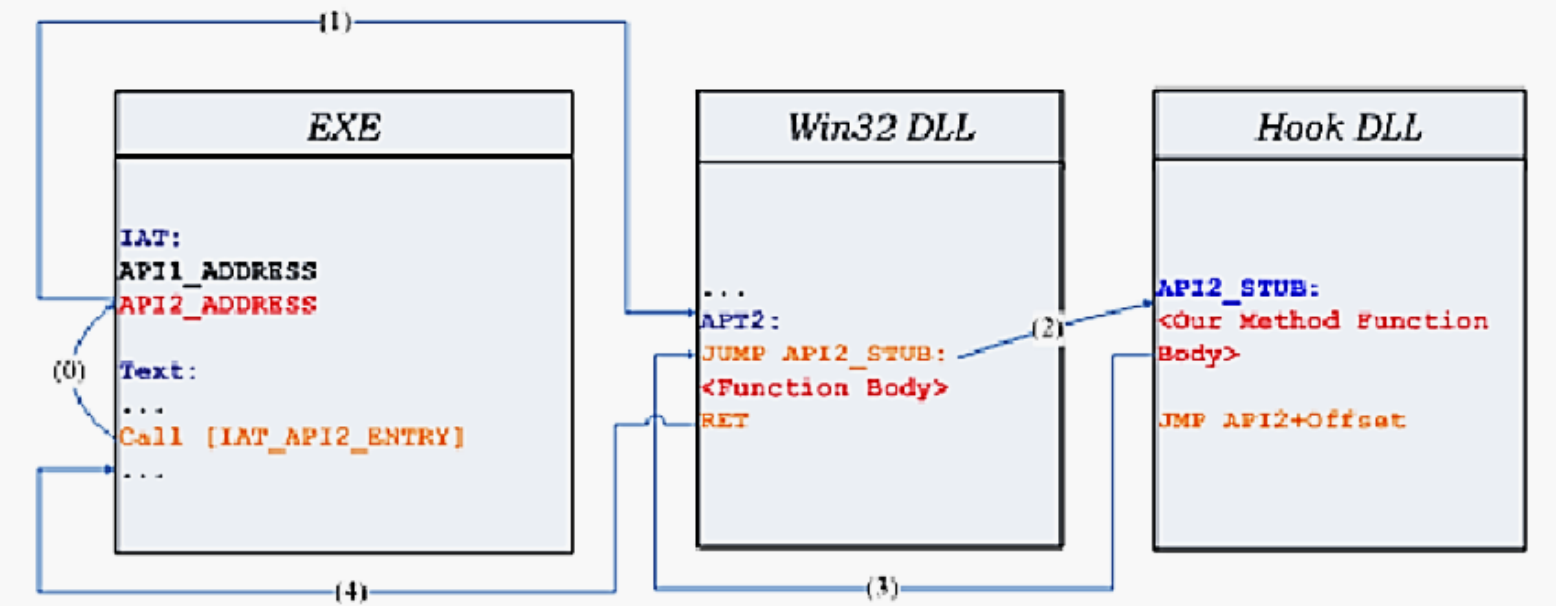


Reasons behind remote thread creation:

- Forcing a breakpoint by a Debugger
- Obtaining internal information from a process (ex: Heap)
- Used for code/DLL injection (ex: API Hooking)

```
HANDLE CreateRemoteThread(
  [in]  HANDLE                 hProcess,
  [in]  LPSECURITY_ATTRIBUTES  lpThreadAttributes,
  [in]  SIZE_T                 dwStackSize,
  [in]  LPTHREAD_START_ROUTINE lpStartAddress,
  [in]  LPVOID                 lpParameter,
  [in]  DWORD                  dwCreationFlags,
  [out] LPDWORD                lpThreadId
);
```

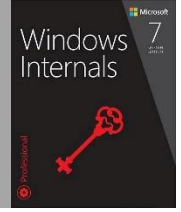
API Hooking



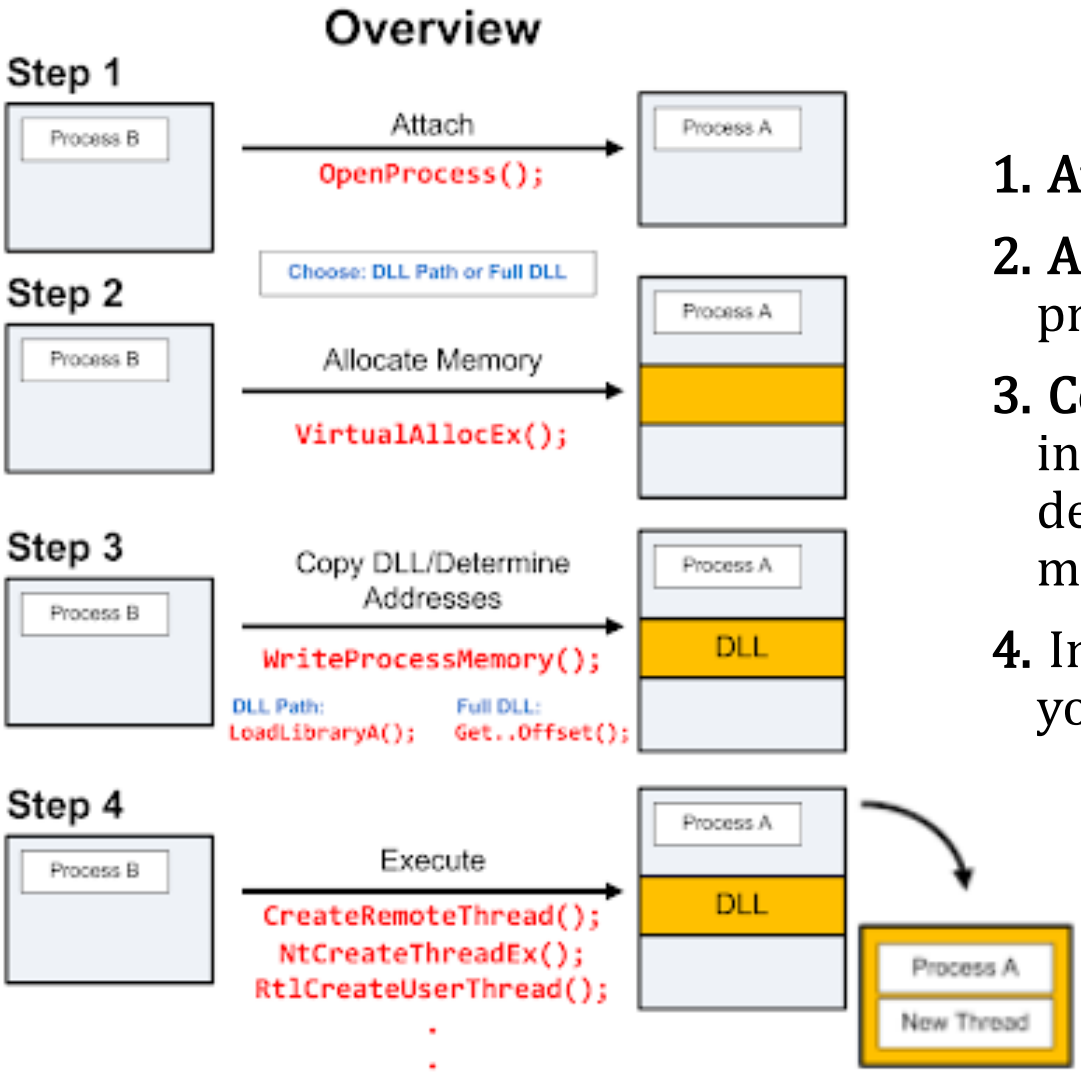
www.researchgate.net

akazemi67

DLL Injection Procedure



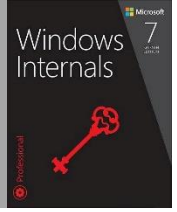
blog.opensecurityresearch.com



1. **Attach** to the process
2. **Allocate** Memory within the process
3. **Copy** the DLL or the DLL Path into the processes memory and determine appropriate memory addresses
4. Instruct the process to **Execute** your DLL

akazemi67

Further Readings



https://www.apriorit.com/dev-blog/679-windows-dll-injection-for-api-hooks

https://m417z.com/Implementing-Global-Injection-and-Hooking-in-Windows/

https://github.com/odzhan/injection

CODING TIME

CODING TIME

DLL Injection

akazemi67