|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| * **Message Hook 의 종류** | | | | |
| **M : Modify R : Remove** | | | | |
| **HOOK** | **Description** | **where** | **M** | **R** |
| WH\_CALLWNDPROC | SendMessage()을 사용해 보내는 메세지를 가로챈다. | Thread or global | X | X |
| WH\_CALLWNDPROCRET | SendMessage()의 리턴값을 가로챈다. | Thread or global |  |  |
| WH\_GETMESSAGE | GetMessage(), PeekMessage()에 호출을 가로 챈다. | Thread or global | O | O |
| WH\_KEYBOARD |  | Thread or global | O | O |
| WH\_KEYBOARD\_LL |  | Global only |  |  |
| WH\_MOUSE |  | Thread or global | O | O |
| WH\_MOUSE\_LL |  | Global only |  |  |
| WH\_FOREGROUNDIDLE |  | Thread or global | X | X |
| WH\_MSGFILTER |  | Thread or global | O | O |
| WH\_SYSMSGFILTER |  | Global only |  |  |
| WH\_SHELL |  | Thread or global |  |  |
| WH\_CBT |  | Thread or global |  |  |
| WH\_JOURNALRECORD |  | Global only | X | X |
| WH\_JOURNALPLAYBACK |  | Global only | X | X |
| WH\_DEBUG |  | Thread or global |  |  |

CreateRemoteThread 함수를 사용해서 DLL을 Injection 할 때는 다음 단계를 따른다.

1. 원하는 프로세스의 핸들을 얻는다.
2. LoadLibraryA()의 주소를 구한다.

질문 – C에서 함수의 이름은 주소를 나타낸다. 위 코드대신 아래 처럼 사용하면 안될까 ?

1. DLL을 넣을 프로세스의 주소 공간에 메모리를 할당하고, DLL의 이름을 복사한다.
2. CreateRemoteThread 함수를 사용해서 새로운 스레드를 생성한다. 이때 함수는 LoadLibraryA 를 수행하게 하고 파라미터로는 DLL의 이름을 담고 있는 메모리 주소를 전달한다.