Injection through Hooking

Hook injection describes a way to load malware that takes advantage of **Windows hooks**, which are used to intercept messages destined for applications. Malware authors can use hook injection to accomplish two things:

- To be sure that malicious code will run whenever a particular message is intercepted
- To be sure that a particular DLL will be loaded in a victim process's memory space

> A hook is a mechanism by which an application can intercept events, such as messages, mouse actions, and keystrokes. A function that intercepts a particular type of event is known as a hook procedure. A hook procedure can act on each event it receives, and then modify or discard the event. The following some example uses for hooks:
>
> - Monitor messages for debugging purposes
> - Provide support for recording and playback of macros
> - Provide support for a help key (F1)
> - Simulate mouse and keyboard input
> - Implement a computer-based training (CBT) application

- The overall flow for preparing the hook to be loaded and executed requires the injector to follow these steps:

> 1. Obtain the target process handle.
> 2. Allocate memory within a target process and write the external DLL path into it (here we mean writing the dynamic library path that contains the hook).
> 3. Create a thread inside the target process that would load the library and set up the hook.