

Forum:[Hack Forums](#)

Thread: [\[JOEBOB'S POST\] Inject DLL before program](#)

Mr. Kim - April 8, 2017, 4:30 pm

User can't post in the proper forum, I'm posting this here on their behalf.

Quote:I'm trying to hook the Direct Input function "DirectInput8Create" but it happens too early so that starting the target program then manually injecting the DLL isn't an option as I would be too late to catch the event.

I know programs like Ollydbg and x64dbg can essentially load a program but stop it from executing on the first line of code until you tell it to start, would something like this be the best option? If so, does anyone have any tips on how to accomplish it? Or is there some better way to handle this?

Thanks.

edit: I found this blog post that helped explain most of what I needed. (can't post links yet)

However I'm a bit stuck on finding the entry point. Using x64dbg to find my program's entry point works great but I get a different value when I try reading the .exe file using the WinNT.h functions and doing:

```
entryPoint = ntHeader->OptionalHeader.ImageBase +  
ntHeader->OptionalHeader.AddressOfEntryPoint;
```

Anyone have any idea why that wouldn't be giving the correct address?