隐藏DLL模块(HideDll)

转载

weixin_33859665 于 2019-07-05 01:47:15 发布 2398 收藏
文章标签： c/c++ 大数据
原文链接：http://www.cnblogs.com/rogee/archive/2011/04/30/2033404.html


```
void HideDll()
{
    HMODULE hMod = ::GetModuleHandle("MyHook.dll");
    PLIST_ENTRY Head,Cur;
    PPEB_LDR_DATA ldr;
    PLDR_MODULE ldm;
    __asm
    {
        mov eax , fs:[0x30]
        mov ecx , [eax + 0x0c] //Ldr
        mov ldr , ecx
    }
    Head = &(ldr->InLoadOrderModuleList);
    Cur = Head->Flink;
    do
    {
        ldm = CONTAINING_RECORD( Cur, LDR_MODULE, InLoadOrderModuleList);
        //printf("EntryPoint [0x%X]\n",ldm->BaseAddress);
        if( hMod == ldm->BaseAddress)
         {
            ldm->InLoadOrderModuleList.Blink->Flink =
                ldm->InLoadOrderModuleList.Flink;
            ldm->InLoadOrderModuleList.Flink->Blink =
                ldm->InLoadOrderModuleList.Blink;
            ldm->InInitializationOrderModuleList.Blink->Flink =
                ldm->InInitializationOrderModuleList.Flink;
            ldm->InInitializationOrderModuleList.Flink->Blink =
                ldm->InInitializationOrderModuleList.Blink;
            ldm->InMemoryOrderModuleList.Blink->Flink =
                ldm->InMemoryOrderModuleList.Flink;
            ldm->InMemoryOrderModuleList.Flink->Blink =
                ldm->InMemoryOrderModuleList.Blink;
            break;
         }
        Cur= Cur->Flink;
     }while(Head != Cur);
}
```

转载于:https://www.cnblogs.com/rogee/archive/2011/04/30/2033404.html