dll注入到 模块中 隐藏外挂模块 接收用户的指令 交互通道

安全保护

隐藏的进程

1、注入注册表 设置键值

2、远线程注入 开启远线程 加载模块CreateRemoteThread LoadLiberary

-把dll路径写入进程 开启远线程 参数为LoadLiberay 和其地址 （容易防御）

3、借用可信任进程 远线程 dll注入到service进程 service调用函数注入到目标进程

卸载service中的dll 遍历进程

4、APC注入 异步过程调用 挂起时 线程插入一个APC QuenueUserAPC

5、消息钩子注入

6、输入表注入

7、创建进程时注入 悬挂 双进程保护

8、LSP注入

9、输入法注入

10、comres注入、

三、隐藏模块

抹掉pe头 断开ldr\_moudle链

四、交互通道 传递输入给dll 消息钩子 hook原有的消息处理过程 获取键状态 进程间通信

五、 call函数 外挂call 防止被检测

1、栈帧检测 检测调用处的返回地址 确定是否非法调用

获取函数地址 getmoudlehandle getprocadrress 将参数入栈然后call

在被调用函数中检测调用 地址 hook ce远线程注入