API HOOK-全局键盘钩子消息实战

1.实验目标

实现拦截全局键盘消息，获得按键字符

2.实验环境

- windows 1909
- VS 2019+Delphi10.3Rio
- DebugView
- 火绒杀毒软件

3.实验注入的DLL代码

```
#include<windows.h>
HHOOK MyHOOK = NULL;
LRESULT CALLBACK MyKeyboardProc(int code, WPARAM wParam, LPARAM lParam) {
    if (wParam == WM_KEYDOWN) {
        PKBDLLHOOKSTRUCT pmykey = (PKBDLLHOOKSTRUCT)lParam;
        DWORD MyKey = pmykey->vkCode;
        CHAR MyBuffer[MAXBYTE];
        wsprintf(MyBuffer, "Key:%c", MyKey);
        OutputDebugString(MyBuffer);
    }
    return CallNextHookEx(MyHOOK,code,wParam,lParam);
}

BOOL SetHOOK() {
    HMODULE MyDll=GetModuleHandle(NULL);
    MyHOOK =SetWindowsHookEx(WH_KEYBOARD_LL,MyKeyboardProc,MyDll,0);
    if (MyHOOK != NULL) {

        return TRUE;
    }
    else {
        return FALSE;
    }
}

BOOL UnSetHOOK() {
    return UnhookWindowsHookEx(MyHOOK);
}
```

DEF文件：

```
LIBRARY
EXPORTS
    SetHOOK
    UnSetHOOK
```

4.窗口界面Delphi代码

```
unit Unit1;

interface

uses
  Winapi.Windows, Winapi.Messages, System.SysUtils, System.Variants,
System.Classes, Vcl.Graphics,
  Vcl.Controls, Vcl.Forms, Vcl.Dialogs, Vcl.StdCtrls;

type
  TForm1 = class(TForm)
    btn1: TButton;
    btn2: TButton;
    procedure btn1Click(Sender: TObject);
    procedure btn2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;
function SetHOOK(): Cardinal;external 'HOOKDLL.dll' name  'SetHOOK';
function UnSetHOOK():Cardinal;external 'HOOKDLL.dll' name  'UnSetHOOK';
implementation

{$R *.dfm}

procedure TForm1.btn1Click(Sender: TObject);
var
temp:Cardinal;
begin
     temp:=SetHOOK();
     if(temp<>0)then
     begin
       ShowMessage('安装成功!');
     end
     else
     begin
       ShowMessage('安装失败!');
     end;
end;

procedure TForm1.btn2Click(Sender: TObject);
var
temp:Cardinal;
begin
     temp:=UnSetHOOK();
     if(temp<>0)then
     begin
       ShowMessage('反安装成功!');
     end
     else
```

```
      begin
        ShowMessage('反安装失败!');
      end;
end;

end.
```

5.实验结果截图