外挂开发

@M了个J

https://weibo.com/exceptions

https://github.com/CoderMJLee

实力IT教育 www.520it.com

小码哥教育 SEEMYGO

外挂演示

- 外挂界面
- 事件处理
- 跨进程访问

小码哥教育 SEEMYGO

外挂界面

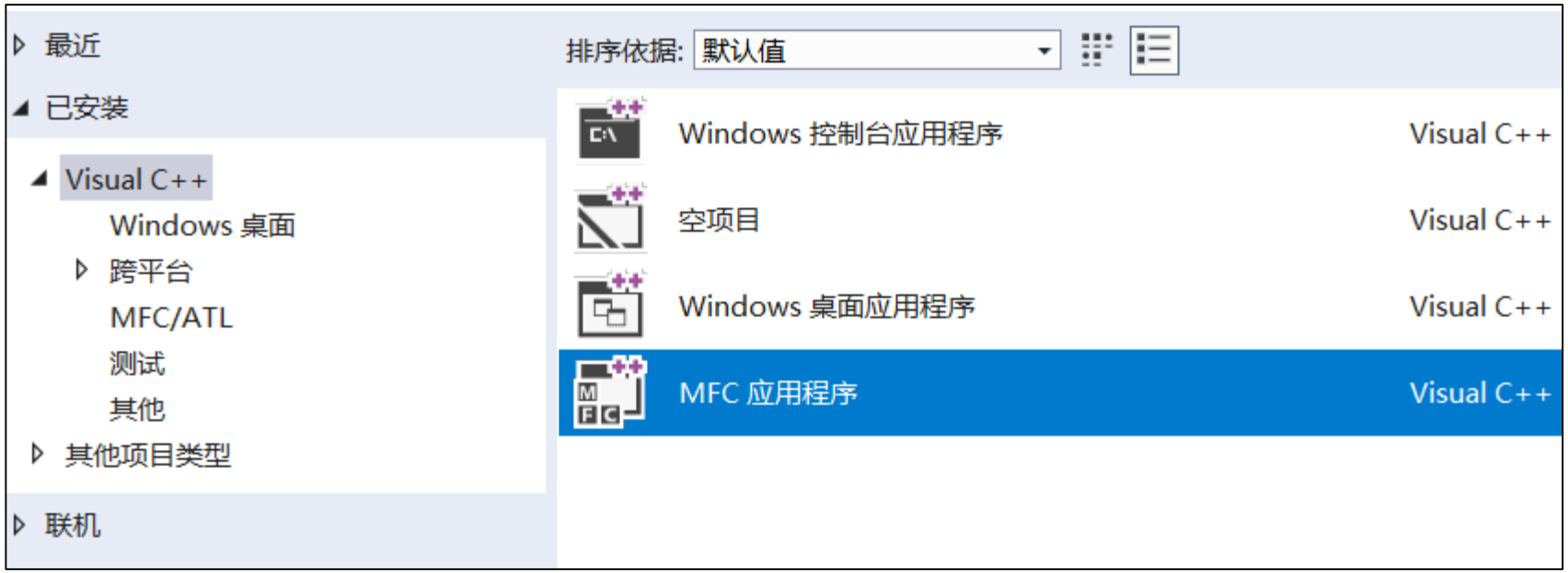
- Windows平台的桌面开发
  - C++：MFC、Qt
  - C#： WinForm、WPF

- 我们课程选用最古老的MFC，不用引入其他外部的框架

- 要先安装好MFC组件

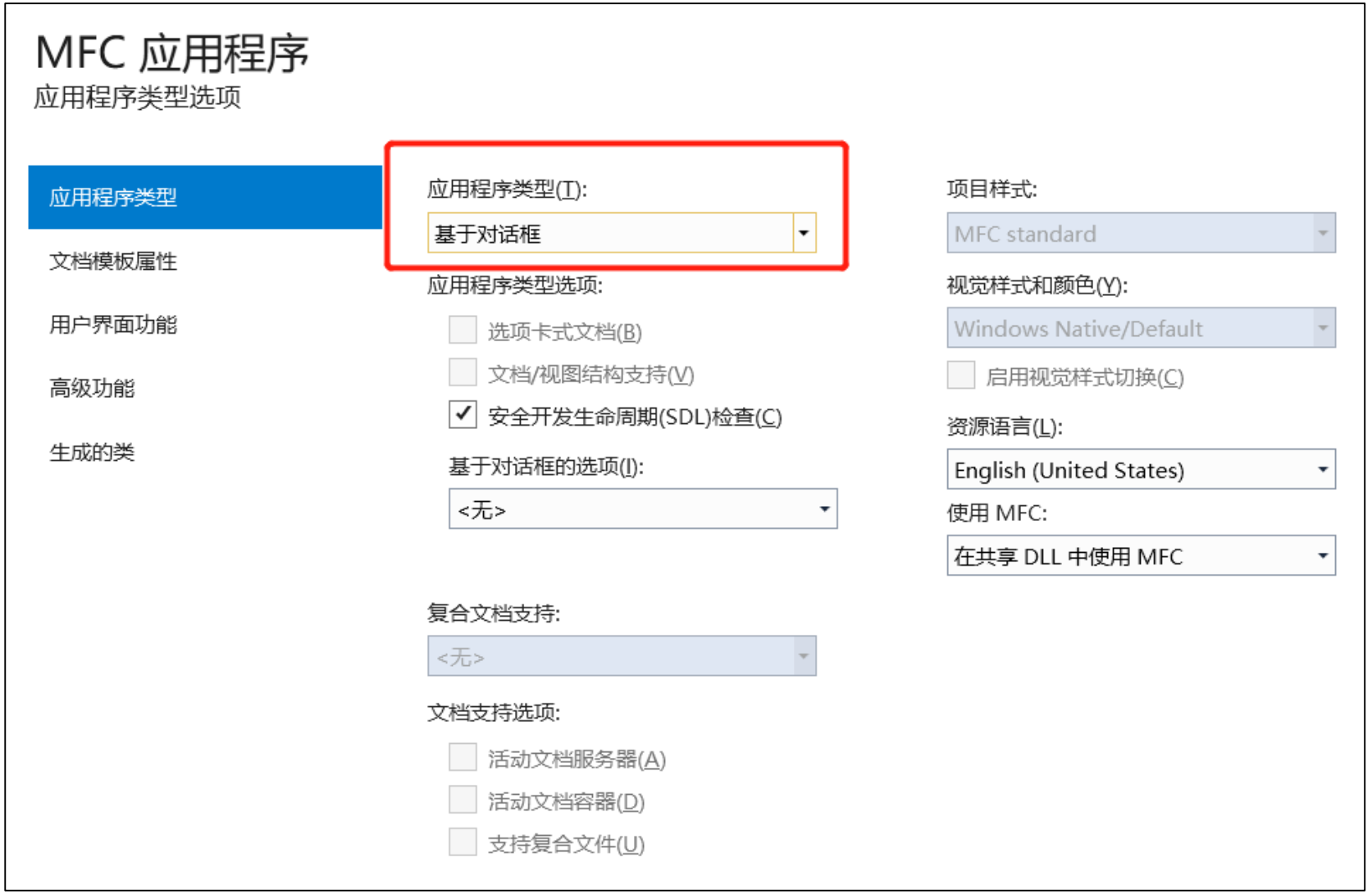
小码哥教育 SEEMYGO

创建MFC项目



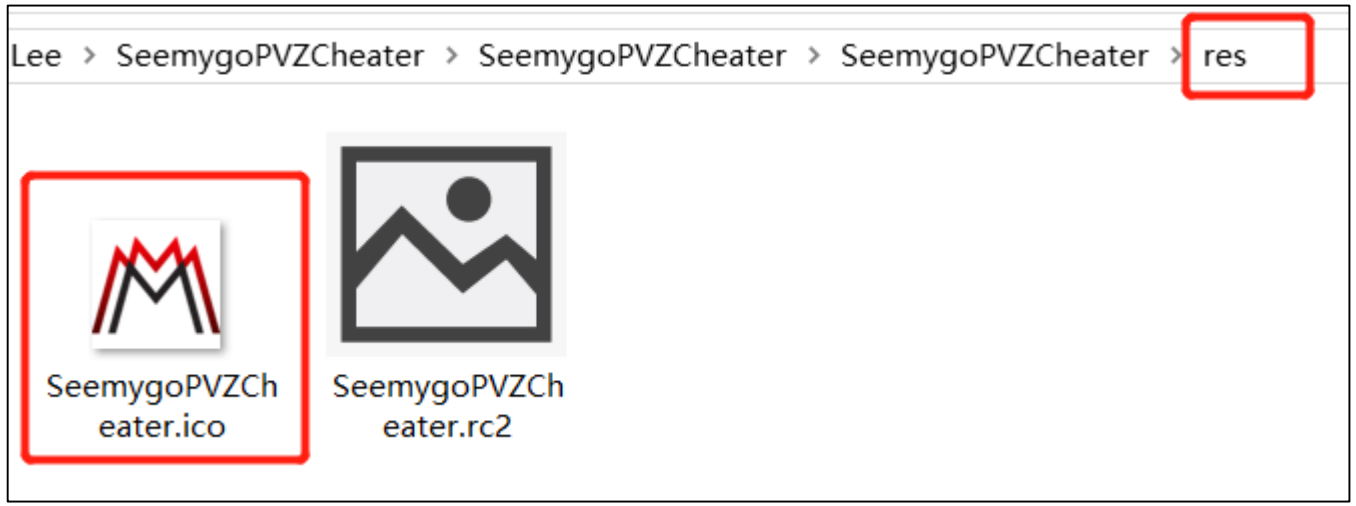
小码哥教育 SEEMYGO

创建MFC项目

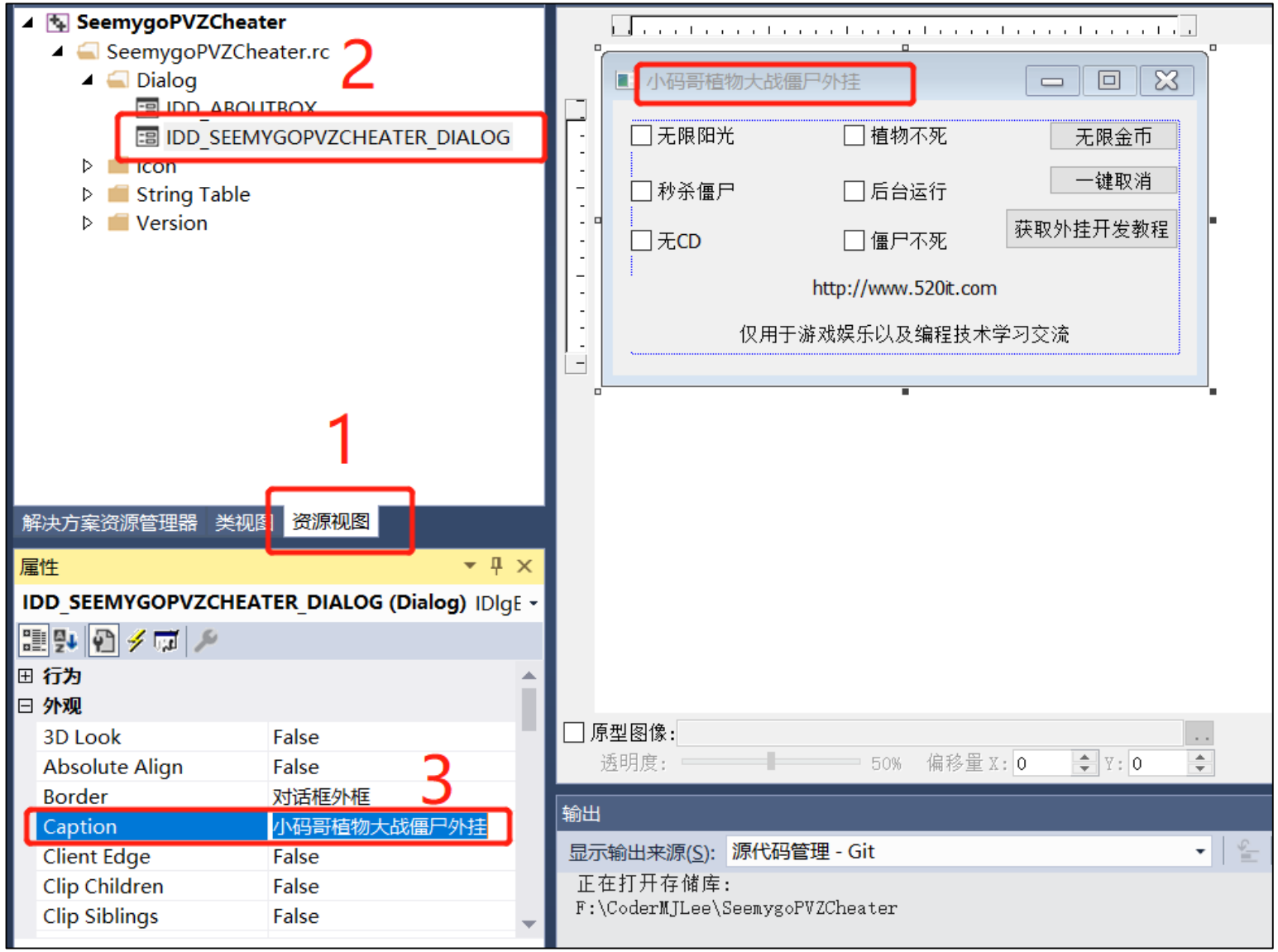


修改LOGO图标

- 替换掉res目录下的ico文件即可



修改窗口标题


SeemygoPVZCheater
SeemygoPVZCheater.rc
Dialog
IDD_ABOUTBOX
IDD_SEEMYGOPVZCHEATER_DIALOG
Icon
String Table
Version
2
1
解决方案资源管理器
类视图
资源视图
属性
IDD_SEEMYGOPVZCHEATER_DIALOG (Dialog) IDlgE
行为
外观
3D Look
False
Absolute Align
False
Border
对话框外框
Caption
小码哥植物大战僵尸外挂
Client Edge
False
Clip Children
False
Clip Siblings
False
3
小码哥植物大战僵尸外挂
无限阳光
植物不死
无限金币
秒杀僵尸
后台运行
一键取消
无CD
僵尸不死
获取外挂开发教程
http://www.520it.com
仅用于游戏娱乐以及编程技术学习交流
原型图像:
透明度:
50%
偏移量 X: 0
Y: 0
输出
显示输出来源(S):
源代码管理 - Git
正在打开存储库:
F:\CoderMJLee\SeemygoPVZCheater

小码哥教育 SEEMYGO

打开工具箱

小码哥教育 SEEMYGO

打印调试

- TRACE函数：类似于C语言的printf，只能在DEBUG调试模式下看到打印信息（F5启动）

```
TRACE("age is %d\n", 20);
```

- AfxMessageBox函数

```
CString str;
str.Format(CString("age is %d"), 20);
AfxMessageBox(str);
```

- MessageBox函数：只在CWnd的子类中使用，功能比AfxMessageBox多

```
CString str;
str.Format(CString("age is %d"), 20);
MessageBox(str);
MessageBox(str, CString("错误"), MB_YESNO | MB_ICONERROR);
```

小码哥教育 SEEMYGO

自定义log宏，简化打印

```
#define log(fmt, ...) \
CString str; \
str.Format(CString(fmt), __VA_ARGS__); \
AfxMessageBox(str);
```

```
log("age is %d", 20);
```

小码哥教育 SEEMYGO

打开URL

```
ShellExecute(
    NULL,
    CString("open"),
    CString("https://ke.qq.com/course/336509"),
    NULL, NULL, SW_SHOWNORMAL);
```

事件注册 – 手动

Resource.h

MFCApplication1 (全局范围)

```
7   #define IDS_ABOUTBOX                    101
8   #define IDD_MFCAPPLICATION1_DIALOG      102
9   #define IDR_MAINFRAME                   128
10  #define IDC_COURSE                      1000
```

MFCApplication1Dlg.h

MFCApplication1 (全局范围)

```
25  protected:
26      HICON m_hIcon;
27
28      // 生成的消息映射函数
29      virtual BOOL OnInitDialog();
30      afx_msg void OnSysCommand(UINT nID, LPARAM lParam);
31      afx_msg void OnPaint();
32      afx_msg HCURSOR OnQueryDragIcon();
33      DECLARE_MESSAGE_MAP()
34  public:
35
36      afx_msg void OnBnClickedCourse();
37  };
38
```

MFCApplication1Dlg.cpp

MFCApplication1 (全局范围)

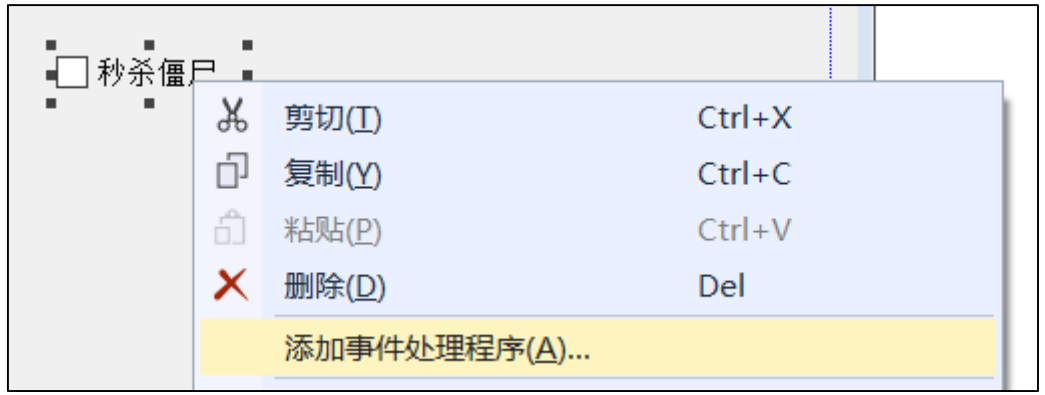
```
163 void CMFCApplication1Dlg::OnBnClickedCourse()
164 {
165
166 }
```

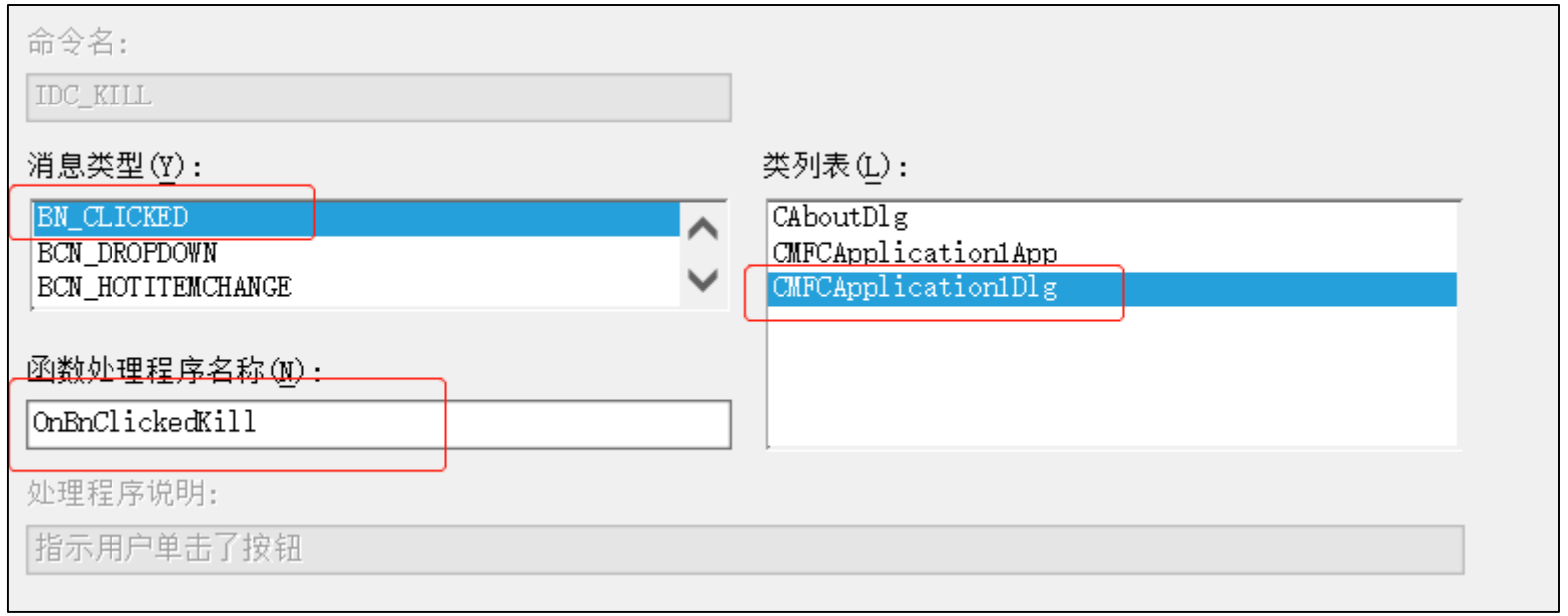
MFCApplication1Dlg.cpp

MFCApplication1 (全局范围)

```
69  BEGIN_MESSAGE_MAP(CMFCApplication1Dlg, CDialogEx)
70      ON_WM_SYSCOMMAND()
71      ON_WM_PAINT()
72      ON_WM_QUERYDRAGICON()
73      ON_BN_CLICKED(IDC_COURSE, &CMFCApplication1Dlg::OnBnClickedCourse)
74  END_MESSAGE_MAP()
```

事件注册 – 自动（也可以直接双击控件）





小码哥教育 SEEMYGO

绑定成员变量 – 手动

MFCApplication1Dlg.h

MFCApplication1

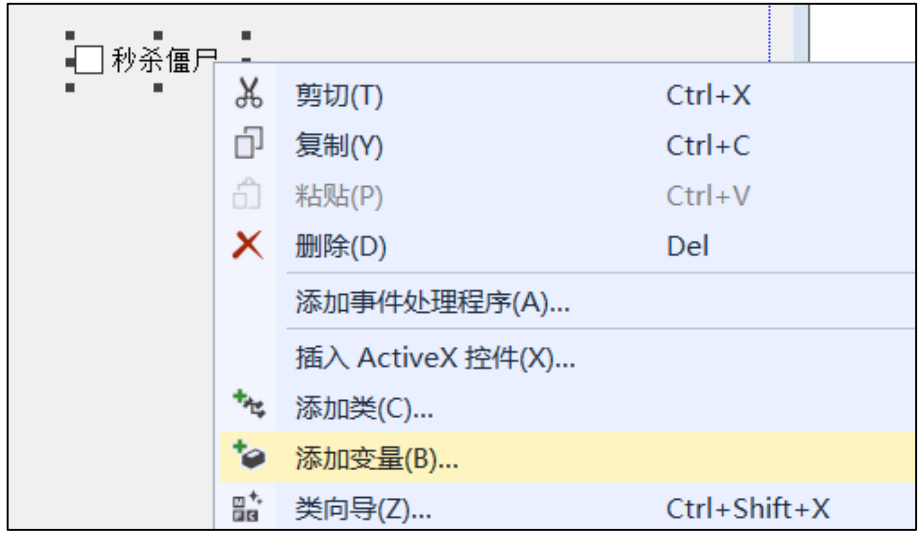
```
40  private:
41      CButton m_sunshine;
42      CButton m_kill;
43  };
```

MFCApplication1Dlg.cpp

MFCApplication1 (全局范围)

```
64  void CMFCApplication1Dlg::DoDataExchange(CDataExchange* pDX)
65  {
66      CDialogEx::DoDataExchange(pDX);
67      DDX_Control(pDX, IDC_SUNSHINE, m_sunshine);
68      DDX_Control(pDX, IDC_KILL, m_kill);
69  }
```

绑定成员变量 – 自动


秒杀僵尸
剪切(T) Ctrl+X
复制(Y) Ctrl+C
粘贴(P) Ctrl+V
删除(D) Del
添加事件处理程序(A)...
插入 ActiveX 控件(X)...
添加类(C)...
添加变量(B)...
类向导(Z)... Ctrl+Shift+X


控件
其他
控件 ID(I):
IDC_KILL
控件类型(Y):
CHECK
类别(T):
控件
名称(N):
m_kill
访问(A):
private
变量类型(V):
CButton
注释(M):
秒杀僵尸

小码哥教育 SEEMYGO

单选框的状态读取和修改 – 方法1

```
// 读取
BOOL state = IsDlgButtonChecked(IDC_SUNSHINE);

// 修改
CheckDlgButton(IDC_SUNSHINE, true);
```

小码哥教育 SEEMYGO

单选框的状态读取和修改 – 方法2

```
CButton *button = (CButton *)GetDlgItem(IDC_SUNSHINE);

// 读取
BOOL state = button->GetCheck();

// 修改
button->SetCheck(true);
```

小码哥教育 SEEMYGO

单选框的状态读取和修改 – 方法3

```
// 读取
BOOL state = this->m_kill.GetCheck();

// 修改
this->m_kill.SetCheck(true);
```

小码哥教育 SEEMYGO

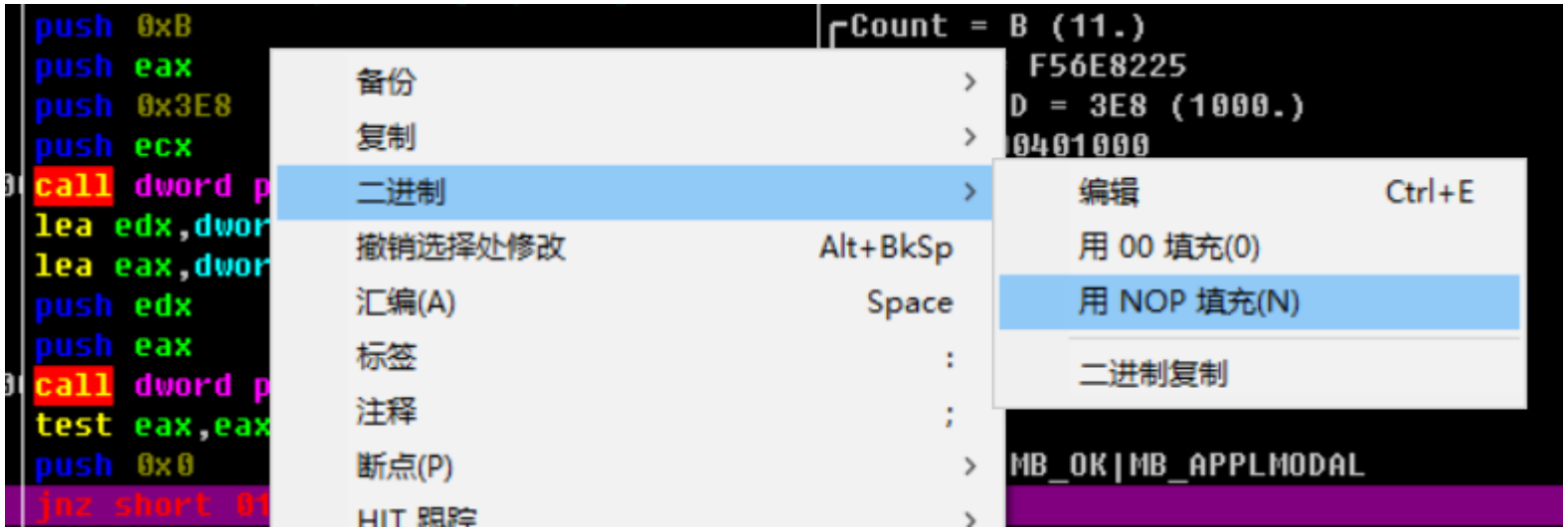
软件破解

- Windows平台软件破解必备知识
  - 文件格式：PE文件
  - 汇编语言：x86、x64汇编
  - 工具：Ollydbg
  - Windows API

- OD常用快捷键
  - F2：切换断点
  - F9：运行程序
  - F7：Step Into
  - F8：Step Over
  - Ctrl + G：搜索代码

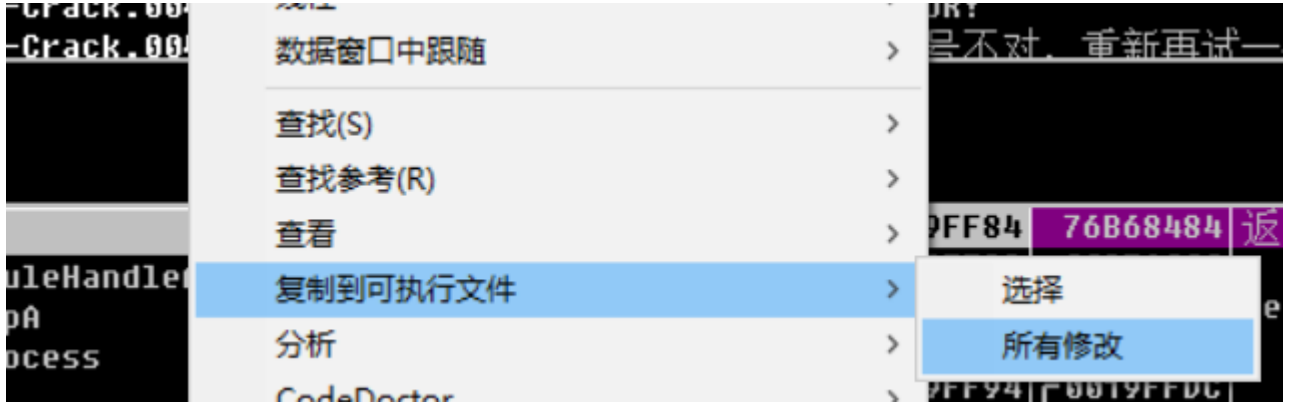
小码哥教育 SEEMYGO

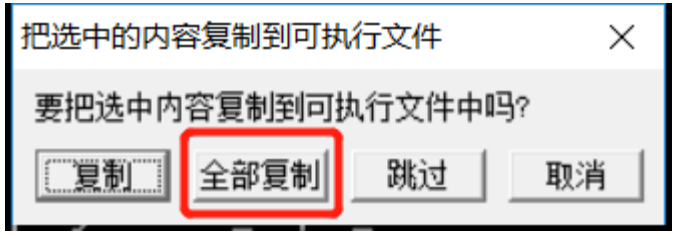
用NOP填充

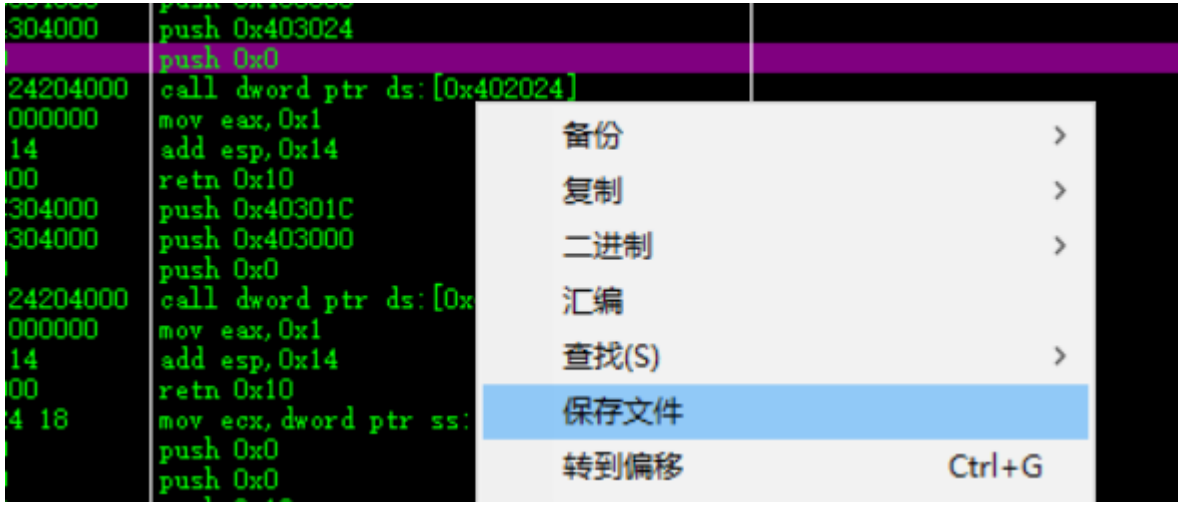


小码哥教育 SEEMYGO

导出破解后的exe文件

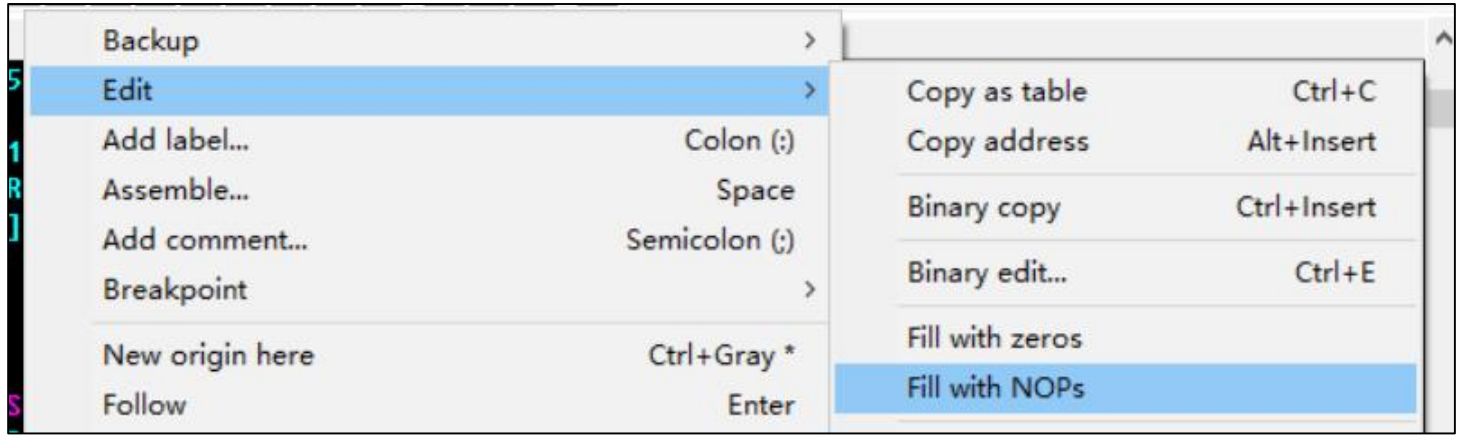


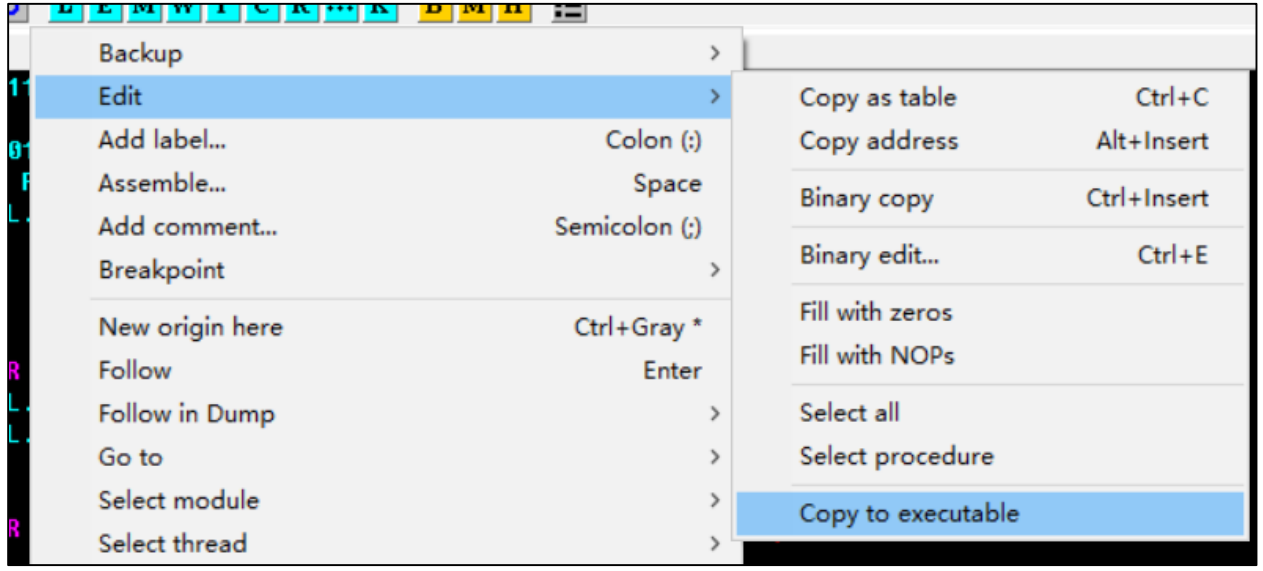




小码哥教育 SEEMYGO

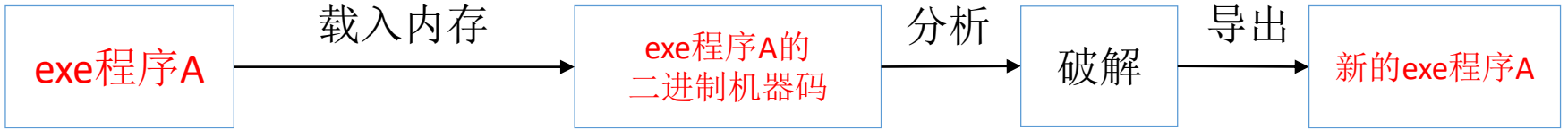
OD 2.0



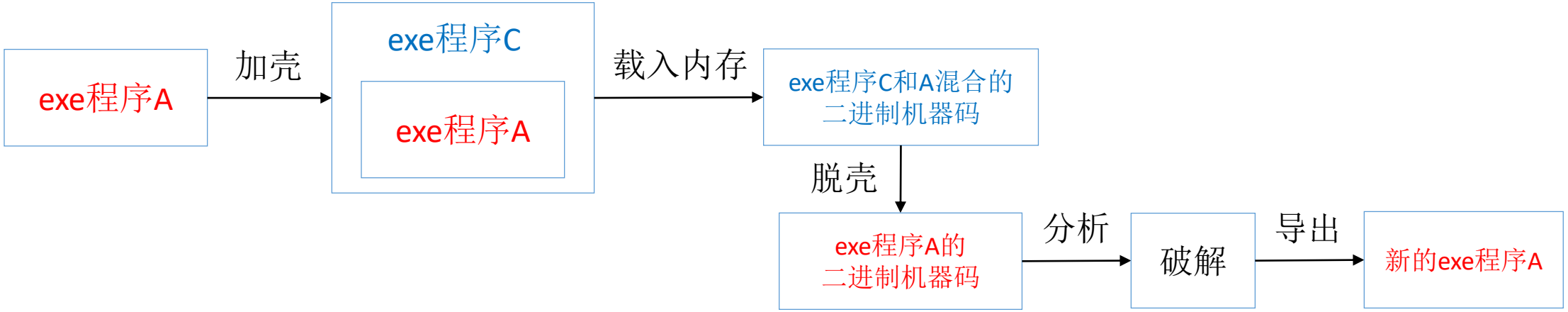


加壳与脱壳

■ 一般的软件破解思路



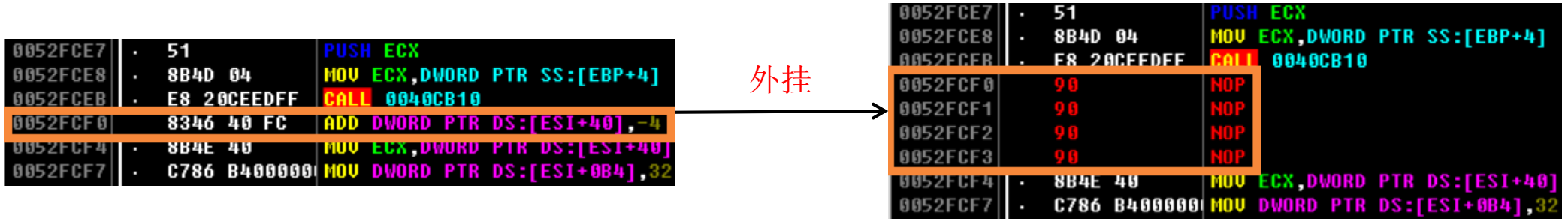
■ 加壳和脱壳



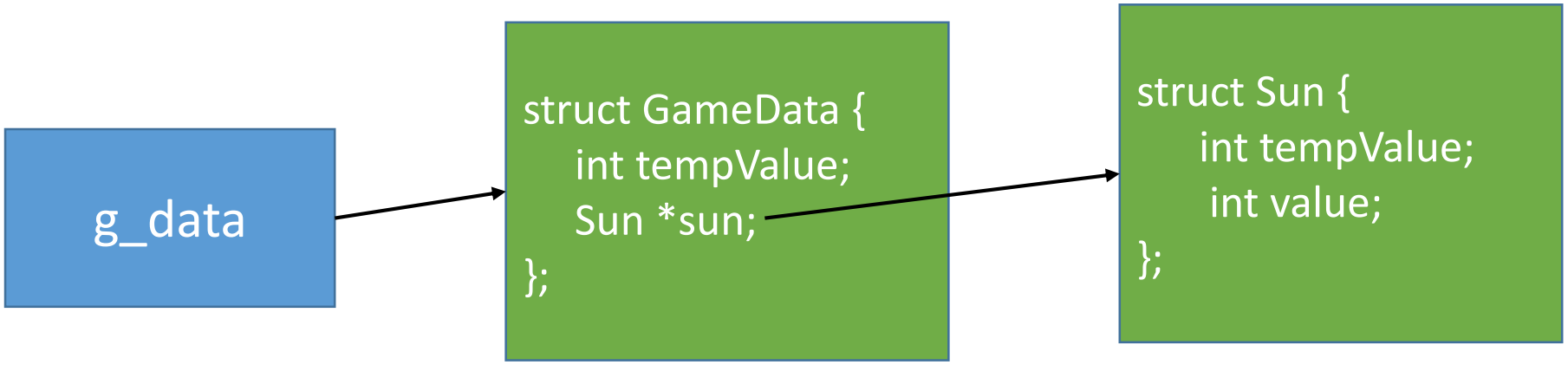
外挂的本质

- 常见的外挂功能有2种做法
  - 修改内存中的数据

  - 修改内存中的代码



- 其实数据和代码并没有本质区别, 在内存中都是0和1


g_data
struct GameData {
int tempValue;
Sun *sun;
};
struct Sun {
int tempValue;
int value;
};

小码哥教育 SEEMYGO

使用Spy++查找窗口