# 加壳器

加。。。

15PB 22期 壳 – 王越卿

# 01 没做的功能

- TLS 处理
- 全部加密压缩
- 花指令

# 02 心得与总结与分享经验

**一个渣渣混淆：**

```
_asm
{
    jmp label1
    label2:
    _emit 0xeb;         // 跳到下边的 CALL
    _emit 0x04;
    CALL DWORD PTR DS : [EAX + EBX * 2 + 0x123402EB];       // 执行 EB 02 也就是跳到下一条指令

    _emit 0xE8;
    _emit 0x00;
    _emit 0x00;
    _emit 0x00;
    _emit 0x00;

                        // 跳到下边的 CALL
    _emit 0xEB;
    _emit 0x0E;

                        // 混淆部分
    PUSH  0x0;
    PUSH  0x0;
    MOV   EAX, DWORD PTR FS : [0];
    PUSH  EAX;

    CALL  DWORD PTR DS : [EAX + EBX * 2 + 0x5019c083];
    push  funcAddress;  // 这里如果是参数传入的需要注意上面的 add eax, ?? 的 ??
    retn;


    jmp   label3
                        // 混淆部分
        _emit 0xE8;
    _emit 0x00;
    _emit 0x00;
    _emit 0x00;
    _emit 0x00;

label1:
    jmp label2;
```

# 02 心得与总结与分享经验

**一个渣渣混淆的效果：**