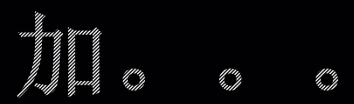
# 加壳器



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;
                                                       // 执行 EB 02 也就是跳到下一条指令
   CALL DWORD PTR DS : [EAX + EBX * 2 + 0x123402EB];
   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;
        0x0;
   VOM
         EAX, DWORD PTR FS : [0];
   PUSH EAX;
   CALL DWORD PTR DS : [EAX + EBX * 2 + 0x5019c083];
        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:
   imp label2;
```

## 02 心得与总结与分享经验

#### 一个渣渣混淆的效果:

