

# 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:

Address	Disassembly	Comment
002DD71E	8B C0	mov eax, eax
002DD720	8B C0	mov eax, eax
002DD722	8B C0	mov eax, eax
002DD724	8B C0	mov eax, eax
002DD726	8B C0	mov eax, eax
002DD728	A1 68 8E 2E 00	mov eax, dword ptr ds:[2E8E68]
002DD72D	89 45 F4	mov dword ptr ss:[ebp-C], eax
002DD730	EB 2F	jmp <test1_fkbug.sub_2DD761>
002DD732	EB 04	jmp test1_fkbug.2DD738
002DD734	3E FF 94 58 EB 02	call dword ptr ds:[eax+ebx*2+123402EB]
002DD73C	E8 00 00 00 00	call <test1_fkbug.sub_2DD741>
002DD741	EB 0E	jmp test1_fkbug.2DD751
002DD743	6A 00	push 0
002DD745	6A 00	push 0
002DD747	64 A1 00 00 00 00	mov eax, dword ptr fs:[0]
002DD74D	50	push eax
002DD74E	3E FF 94 58 83 C0	call dword ptr ds:[eax+ebx*2+5019C083]
002DD756	FF 75 F4	push dword ptr ss:[ebp-C]
002DD759	C3	ret
002DD75A	EB 07	jmp test1_fkbug.2DD763
002DD75C	E8 00 00 00 00	call <test1_fkbug.sub_2DD761>
002DD761	EB CF	jmp test1_fkbug.2DD732
002DD763	5F	pop edi