mvm 防御

整数溢出，将检测*((_QWORD)j + 1) > 6的jle patch为jbe即可。

diff 防御

read函数会造成栈溢出，将read的参数从128patch为123即可。

```
unsigned __int64 __fastcall sub_1566(__int64 a1, __int64 a2)
{
  int v3; // [rsp+1Ch] [rbp-14h] BYREF
  void *buf; // [rsp+20h] [rbp-10h]
  unsigned __int64 v5; // [rsp+28h] [rbp-8h]

  v5 = __readfsqword(0x28u);
  v3 = 1;
  printf("file 1 or 2:");
  __isoc99_scanf("%d", &v3);
  if ( v3 == 1 )
  {
    buf = (void *)(a1 + 5);
  }
  else
  {
    if ( v3 != 2 )
      return __readfsqword(0x28u) ^ v5;
    buf = (void *)(a2 + 5);
  }
  printf("filename:");
  read(0, buf, 123uLL);
```

szp2 防御

用 https://github.com/TTY-flag/evilPatcher 上的工具加通防即可。

```
python2 evilPatcher/evilPatcher.py ./szp2 evilPatcher/sandboxs/mini_sandbox.asm
```