Windows Software

Windbg + Mona

```
Program Files (x86)\Common Files\microsoft shared\VC>regsvr32 msdia90.dll
\Windbg86>symchk /r c:\windows\system32\ntdll.dll /s
SRV*c:\symbols*http://msdl.microsoft.com/download/symbols
```

```
.load pykd.pyd
!py mona modules
!py mona config -set workingfoler c:\_c\mona

!py mona.py find -s '\xff\xe4' -m
# ffe4 -> jmp esp

mona.py stackpivot -distance 2221,2800
# 0x0044adec : {pivot 2260 / 0x8d4} :  # MOV DWORD PTR FS:[0],ECX # ADD
ESP,8D4 # RETN    ** [DevManBE.exe] **   |  startnull {PAGE_EXECUTE_READ}
```