EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C80 ESP = 0018FEA8 EBP = 0018FF88

EFL = 00000246

push ebp -》ebp入棧 ESP-4

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C81 ESP = 0018FEA4 EBP = 0018FF88

EFL = 00000246

mov ebp,esp-》EBP= ESP

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C83 ESP = 0018FEA4 EBP = 0018FEA4

EFL = 00000246

sub esp,0C0h-》esp-0C0H

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C89 ESP = 0018FDE4 EBP = 0018FEA4

EFL = 00000206 標誌寄存器 ZF(零值標誌=0)

push ebx -》ebx入棧 esp-4

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C8A ESP = 0018FDE0 EBP = 0018FEA4

EFL = 00000206

push esi -》esi入棧esp-4

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C8B ESP = 0018FDDC EBP = 0018FEA4

EFL = 00000206

push edi -》edi入棧 esp-4

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C8C ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000206

lea edi,[ebp-0C0h] 讀取

EAX = 003E2178 EBX = 7EFDE000 ECX = 003E20D0

EDX = 00000001 ESI = 00000000 EDI = 0018FDE4

EIP = 00411C92 ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000206

mov ecx,30h

EAX = 003E2178 EBX = 7EFDE000 ECX = 00000030

EDX = 00000001 ESI = 00000000 EDI = 0018FDE4

EIP = 00411C97 ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000206

mov eax,0CCCCCCCCh

EAX = CCCCCCCC EBX = 7EFDE000 ECX = 00000030

EDX = 00000001 ESI = 00000000 EDI = 0018FDE4

EIP = 00411C9C ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000206

rep stos dword ptr [edi]

EAX = CCCCCCCC EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 0018FEA4

EIP = 00411C9E ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000206

xor eax,eax

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 0018FEA4

EIP = 00411CA0 ESP = 0018FDD8 EBP = 0018FEA4

EFL = 00000246 標誌寄存器 ZF(零值標誌=1)

pop edi

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411CA1 ESP = 0018FDDC EBP = 0018FEA4

EFL = 00000246

pop esi

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411CA2 ESP = 0018FDE0 EBP = 0018FEA4

EFL = 00000246

pop ebx

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411CA3 ESP = 0018FDE4 EBP = 0018FEA4

EFL = 00000246

mov esp,ebp

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411CA5 ESP = 0018FEA4 EBP = 0018FEA4

EFL = 00000246

pop ebp

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411CA6 ESP = 0018FEA8 EBP = 0018FF88

EFL = 00000246

ret

EAX = 00000000 EBX = 7EFDE000 ECX = 00000000

EDX = 00000001 ESI = 00000000 EDI = 00000000

EIP = 00411C00 ESP = 0018FEAC EBP = 0018FF88

EFL = 00000246

esp：0x0018fde4 -》 00 00 00 00

push ebx （0x7efde000）

esp：0x0018fde0 -》00 e0 fd 7e

push esi 0x00000000

esp: 0x0018fddC ->00 00 00 00 / 00 e0 fd 7e

push edi 0x00000000

esp:0x0018fdd8 ->->00 00 00 00/ 00 00 00 00/ 00 e0 fd 7e

0x0018fea4

**EFL标志位：**

