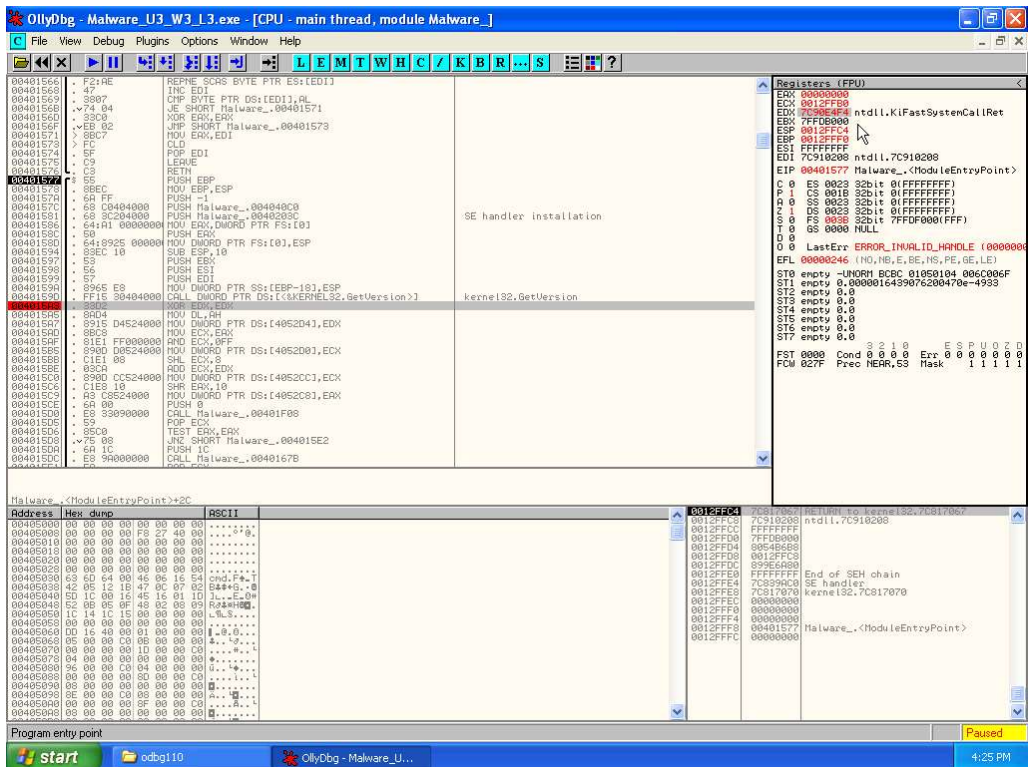
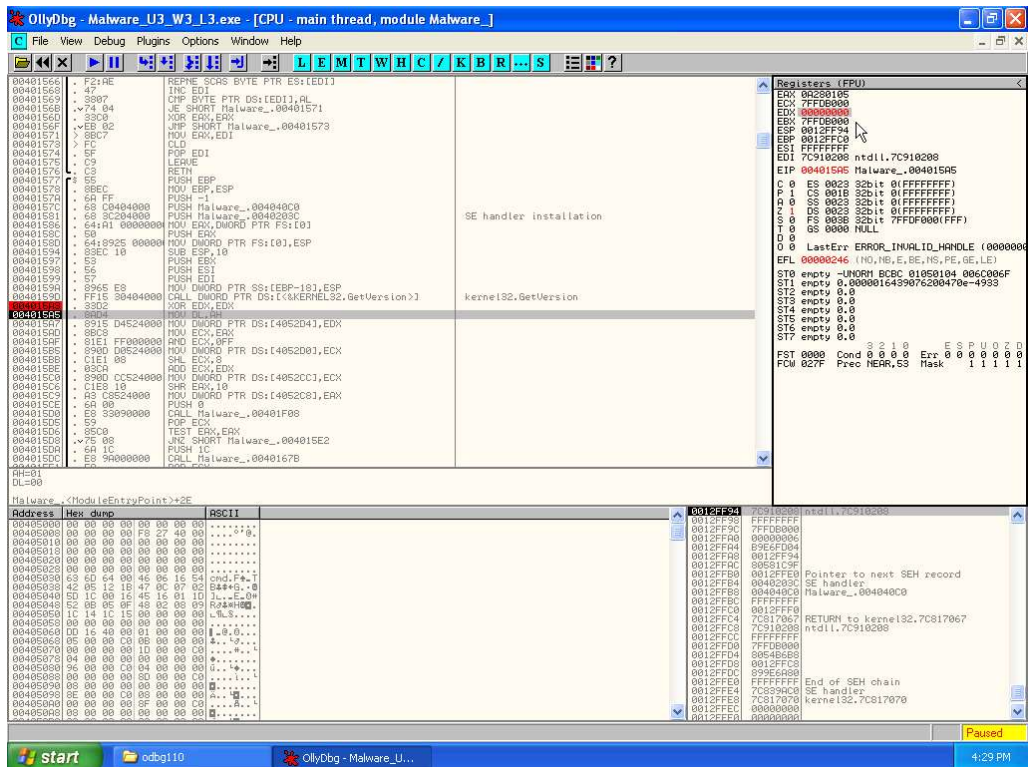


Il valore che viene passato sullo stack dal parametro **CommandLine** è **cmd** (indirizzo 00401067).

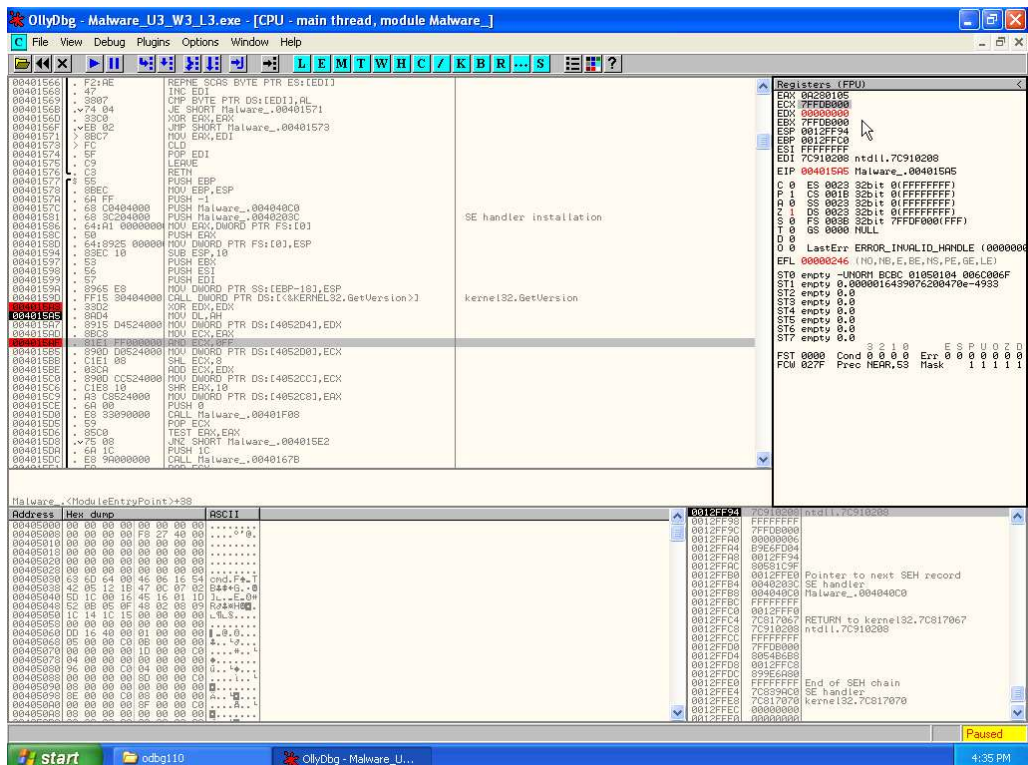


Il valore del registro **EDX** (indirizzo 004015A3) è **7C90EA4F4**.

Creiamo un **breakpoint** ed eseguiamo uno **step-into** e rincontrolliamo il valore del registro **EDX**.



Il nuovo valore è **00000000**. Questo perché lo **XOR** moltiplicato per se stesso non può che ritornare valore **0**. Inseriamo un secondo **breakpoint** all'indirizzo **004015A3** e controlliamo il valore di **ECX**.



Annotiamo il valore (7FFDB000) e facciamo un secondo step-into.

Notiamo che viene eseguita l'istruzione **AND ECX, OFF** ed il valore di **ECX** cambia in **00000001** che non è altro che il risultato del calcolo d'istruzione dei due esadecimali espresso in binario.

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Plugins Options Window Help

LEMTWHC/KBR...S

00401566: REPNE SCAS BYTE PTR ES:[EDI]
00401567: INC EDI
00401568: CMP BYTE PTR DS:[EDI],AL
00401569: JE SHORT Malware_..00401571
0040156A: XOR EAX, EAX
0040156B: JMP SHORT Malware_..00401573
0040156C: > SBC ECX
0040156D: MOV EAX, EDI
0040156E: POP EDI
0040156F: LEAVE
00401570: RETN
00401571: PUSH EBP
00401572: MOV ESP, ESP
00401573: PUSH -1
00401574: PUSH Malware_..004040C0
00401575: PUSH Malware_..0040203C
00401576: MOV EAX, DWORD PTR FS:[0],ESP
00401577: PUSH EAX
00401578: SUB ESP, 10
00401579: PUSH EAX
0040157A: PUSH EAX
0040157B: PUSH EAX
0040157C: CALL DWORD PTR DS:[EBP-10],ESP
0040157D: FF15 30404000
0040157E: XOR EDI, EDI
0040157F: MOV EDI, EDI
00401580: MOV DWORD PTR DS:[4052D4], EDI
00401581: MOV ECX, EAX
00401582: AND ECX, 0FF
00401583: MOV DWORD PTR DS:[4052D0], ECX
00401584: C1E1 08
00401585: SHL ECX, 8
00401586: MOV ECX, EDI
00401587: MOV DWORD PTR DS:[4052CC], ECX
00401588: C1E8 10
00401589: SHR EAX, 10
0040158A: MOV DWORD PTR DS:[4052C8], EAX
0040158B: PUSH 0
0040158C: CALL Malware_..00401F08
0040158D: POP ECX
0040158E: TEST EAX, EAX
0040158F: JNZ SHORT Malware_..004015E2
00401590: MOV ECX, EDI
00401591: CALL Malware_..00401678
00401592: CCM C0

SE handler installation

kernel32.GetVersion

Registers (FPU)

EAX: 00000005
ECX: 00000005
EDX: 00000001
EBX: 77F10000
ESP: 0012FF94
EBP: 0012FFD0
ESI: FFFFFFFF
EDI: 7C910208
EIP: 00401585 Malware_..00401585
C 0 ES 0023 32bit 0 (FFFFFFFF)
P 1 CS 001B 32bit 0 (FFFFFFFF)
A 0 SS 0023 32bit 0 (FFFFFFFF)
C 0 DS 0023 32bit 0 (FFFFFFFF)
S 0 FS 0026 32bit 7 (FFFFFFFF)
T 0 GS 0000 NULL
0 0 LastErr ERROR_INVALID_HANDLE (00000000)
EFL 00000206 (NO, NB, NE, A, NS, PE, GE, G)
ST0 empty -UNORN BCD 01050104 006C006F
ST1 empty 0.0000016439075200470e-4953
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
3 2 1 0 E S P U O Z D
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0
FCW 027F Prec NEAR, SS Itask 1 1 1 1

Malware_..<ModuleEntryPoint>+38

Address Hex Dump ASCII

00405000 00 00 00 00 00 00 00 00
00405005 00 00 00 00 FS 27 40 00 00
00405010 00 00 00 00 00 00 00 00
00405015 00 00 00 00 00 00 00 00
00405020 00 00 00 00 00 00 00 00
00405025 00 00 00 00 00 00 00 00
00405030 63 5D 54 00 46 06 16 54 cond.P=...
00405035 42 05 12 18 47 0C 07 02 0A**0..0
00405040 5D 1C 00 16 45 16 01 1D J...E-0h
00405045 52 06 05 0F 48 02 00 07 8A**000
00405050 1C 14 1C 15 00 00 00 00 %S....
00405055 00 00 00 00 00 00 00 00
00405060 1D 16 40 00 01 00 00 00 I..0..
00405065 05 00 C0 0B 00 00 00 00 ...J..
00405070 00 00 00 00 1D 00 C0 C0 ...W..
00405075 04 00 00 00 00 00 00 00
00405080 56 00 00 C0 04 00 00 00 ...*..
00405085 00 00 00 00 8D 00 00 C0
00405090 05 00 00 00 00 00 00 00
00405095 3E 00 00 C0 03 00 00 00 ..W..
004050A0 00 00 00 00 5F 00 00 C0
004050A5 00 00 00 00 00 00 00 00
004050B0 00 00 00 00 00 00 00 00
004050B5 00 00 00 00 00 00 00 00
004050C0 00 00 00 00 00 00 00 00
004050C5 00 00 00 00 00 00 00 00
004050D0 00 00 00 00 00 00 00 00
004050D5 00 00 00 00 00 00 00 00
004050E0 00 00 00 00 00 00 00 00
004050E5 00 00 00 00 00 00 00 00
004050F0 00 00 00 00 00 00 00 00
004050F5 00 00 00 00 00 00 00 00
00405100 00 00 00 00 00 00 00 00
00405105 00 00 00 00 00 00 00 00
00405110 00 00 00 00 00 00 00 00
00405115 00 00 00 00 00 00 00 00
00405120 00 00 00 00 00 00 00 00
00405125 00 00 00 00 00 00 00 00
00405130 00 00 00 00 00 00 00 00
00405135 00 00 00 00 00 00 00 00
00405140 00 00 00 00 00 00 00 00
00405145 00 00 00 00 00 00 00 00
00405150 00 00 00 00 00 00 00 00
00405155 00 00 00 00 00 00 00 00
00405160 00 00 00 00 00 00 00 00
00405165 00 00 00 00 00 00 00 00
00405170 00 00 00 00 00 00 00 00
00405175 00 00 00 00 00 00 00 00
00405180 00 00 00 00 00 00 00 00
00405185 00 00 00 00 00 00 00 00
00405190 00 00 00 00 00 00 00 00
00405195 00 00 00 00 00 00 00 00
004051A0 00 00 00 00 00 00 00 00
004051A5 00 00 00 00 00 00 00 00
004051B0 00 00 00 00 00 00 00 00
004051B5 00 00 00 00 00 00 00 00
004051C0 00 00 00 00 00 00 00 00
004051C5 00 00 00 00 00 00 00 00
004051D0 00 00 00 00 00 00 00 00
004051D5 00 00 00 00 00 00 00 00
004051E0 00 00 00 00 00 00 00 00
004051E5 00 00 00 00 00 00 00 00
004051F0 00 00 00 00 00 00 00 00
004051F5 00 00 00 00 00 00 00 00
00405200 00 00 00 00 00 00 00 00
00405205 00 00 00 00 00 00 00 00
00405210 00 00 00 00 00 00 00 00
00405215 00 00 00 00 00 00 00 00
00405220 00 00 00 00 00 00 00 00
00405225 00 00 00 00 00 00 00 00
00405230 00 00 00 00 00 00 00 00
00405235 00 00 00 00 00 00 00 00
00405240 00 00 00 00 00 00 00 00
00405245 00 00 00 00 00 00 00 00
00405250 00 00 00 00 00 00 00 00
00405255 00 00 00 00 00 00 00 00
00405260 00 00 00 00 00 00 00 00
00405265 00 00 00 00 00 00 00 00
00405270 00 00 00 00 00 00 00 00
00405275 00 00 00 00 00 00 00 00
00405280 00 00 00 00 00 00 00 00
00405285 00 00 00 00 00 00 00 00
00405290 00 00 00 00 00 00 00 00
00405295 00 00 00 00 00 00 00 00
004052A0 00 00 00 00 00 00 00 00
004052A5 00 00 00 00 00 00 00 00
004052B0 00 00 00 00 00 00 00 00
004052B5 00 00 00 00 00 00 00 00
004052C0 00 00 00 00 00 00 00 00
004052C5 00 00 00 00 00 00 00 00
004052D0 00 00 00 00 00 00 00 00
004052D5 00 00 00 00 00 00 00 00
004052E0 00 00 00 00 00 00 00 00
004052E5 00 00 00 00 00 00 00 00
004052F0 00 00 00 00 00 00 00 00
004052F5 00 00 00 00 00 00 00 00
00405300 00 00 00 00 00 00 00 00
00405305 00 00 00 00 00 00 00 00
00405310 00 00 00 00 00 00 00 00
00405315 00 00 00 00 00 00 00 00
00405320 00 00 00 00 00 00 00 00
00405325 00 00 00 00 00 00 00 00
00405330 00 00 00 00 00 00 00 00
00405335 00 00 00 00 00 00 00 00
00405340 00 00 00 00 00 00 00 00
00405345 00 00 00 00 00 00 00 00
00405350 00 00 00 00 00 00 00 00
00405355 00 00 00 00 00 00 00 00
00405360 00 00 00 00 00 00 00 00
00405365 00 00 00 00 00 00 00 00
00405370 00 00 00 00 00 00 00 00
00405375 00 00 00 00 00 00 00 00
00405380 00 00 00 00 00 00 00 00
00405385 00 00 00 00 00 00 00 00
00405390 00 00 00 00 00 00 00 00
00405395 00 00 00 00 00 00 00 00
004053A0 00 00 00 00 00 00 00 00
004053A5 00 00 00 00 00 00 00 00
004053B0 00 00 00 00 00 00 00 00
004053B5 00 00 00 00 00 00 00 00
004053C0 00 00 00 00 00 00 00 00
004053C5 00 00 00 00 00 00 00 00
004053D0 00 00 00 00 00 00 00 00
004053D5 00 00 00 00 00 00 00 00
004053E0 00 00 00 00 00 00 00 00
004053E5 00 00 00 00 00 00 00 00
004053F0 00 00 00 00 00 00 00 00
004053F5 00 00 00 00 00 00 00 00
00405400 00 00 00 00 00 00 00 00
00405405 00 00 00 00 00 00 00 00
00405410 00 00 00 00 00 00 00 00
00405415 00 00 00 00 00 00 00 00
00405420 00 00 00 00 00 00 00 00
00405425 00 00 00 00 00 00 00 00
00405430 00 00 00 00 00 00 00 00
00405435 00 00 00 00 00 00 00 00
00405440 00 00 00 00 00 00 00 00
00405445 00 00 00 00 00 00 00 00
00405450 00 00 00 00 00 00 00 00
00405455 00 00 00 00 00 00 00 00
00405460 00 00 00 00 00 00 00 00
00405465 00 00 00 00 00 00 00 00
00405470 00 00 00 00 00 00 00 00
00405475 00 00 00 00 00 00 00 00
00405480 00 00 00 00 00 00 00 00
00405485 00 00 00 00 00 00 00 00
00405490 00 00 00 00 00 00 00 00
00405495 00 00 00 00 00 00 00 00
004054A0 00 00 00 00 00 00 00 00
004054A5 00 00 00 00 00 00 00 00
004054B0 00 00 00 00 00 00 00 00
004054B5 00 00 00 00 00 00 00 00
004054C0 00 00 00 00 00 00 00 00
004054C5 00 00 00 00 00 00 00 00
004054D0 00 00 00 00 00 00 00 00
004054D5 00 00 00 00 00 00 00 00
004054E0 00 00 00 00 00 00 00 00
004054E5 00 00 00 00 00 00 00 00
004054F0 00 00 00 00 00 00 00 00
004054F5 00 00 00 00 00 00 00 00
00405500 00 00 00 00 00 00 00 00
00405505 00 00 00 00 00 00 00 00
00405510 00 00 00 00 00 00 00 00
00405515 00 00 00 00 00 00 00 00
00405520 00 00 00 00 00 00 00 00
00405525 00 00 00 00 00 00 00 00
00405530 00 00 00 00 00 00 00 00
00405535 00 00 00 00 00 00 00 00
00405540 00 00 00 00 00 00 00 00
00405545 00 00 00 00 00 00 00 00
00405550 00 00 00 00 00 00 00 00
00405555 00 00 00 00 00 00 00 00
00405560 00 00 00 00 00 00 00 00
00405565 00 00 00 00 00 00 00 00
00405570 00 00 00 00 00 00 00 00
00405575 00 00 00 00 00 00 00 00
00405580 00 00 00 00 00 00 00 00
00405585 00 00 00 00 00 00 00 00
00405590 00 00 00 00 00 00 00 00
00405595 00 00 00 00 00 00 00 00
004055A0 00 00 00 00 00 00 00 00
004055A5 00 00 00 00 00 00 00 00
004055B0 00 00 00 00 00 00 00 00
004055B5 00 00 00 00 00 00 00 00
004055C0 00 00 00 00 00 00 00 00
004055C5 00 00 00 00 00 00 00 00
004055D0 00 00 00 00 00 00 00 00
004055D5 00 00 00 00 00 00 00 00
004055E0 00 00 00 00 00 00 00 00
004055E5 00 00 00 00 00 00 00 00
004055F0 00 00 00 00 00 00 00 00
004055F5 00 00 00 00 00 00 00 00
00405600 00 00 00 00 00 00 00 00
00405605 00 00 00 00 00 00 00 00
00405610 00 00 00 00 00 00 00 00
00405615 00 00 00 00 00 00 00 00
00405620 00 00 00 00 00 00 00 00
00405625 00 00 00 00 00 00 00 00
00405630 00 00 00 00 00 00 00 00
00405635 00 00 00 00 00 00 00 00
00405640 00 00 00 00 00 00 00 00
00405645 00 00 00 00 00 00 00 00
00405650 00 00 00 00 00 00 00 00
00405655 00 00 00 00 00 00 00 00
00405660 00 00 00 00 00 00 00 00
00405665 00 00 00 00 00 00 00 00
00405670 00 00 00 00 00 00 00 00
00405675 00 00 00 00 00 00 00 00
00405680 00 00 00 00 00 00 00 00
00405685 00 00 00 00 00 00 00 00
00405690 00 00 00 00 00 00 00 00
00405695 00 00 00 00 00 00 00 00
004056A0 00 00 00 00 00 00 00 00
004056A5 00 00 00 00 00 00 00 00
004056B0 00 00 00 00 00 00 00 00
004056B5 00 00 00 00 00 00 00 00
004056C0 00 00 00 00 00 00 00 00
004056C5 00 00 00 00 00 00 00 00
004056D0 00 00 00 00 00 00 00 00
004056D5 00 00 00 00 00 00 00 00
004056E0 00 00 00 00 00 00 00 00
004056E5 00 00 00 00 00 00 00 00
004056F0 00 00 00 00 00 00 00 00
004056F5 00 00 00 00 00 00 00 00
00405700 00 00 00 00 00 00 00 00
00405705 00 00 00 00 00 00 00 00
00405710 00 00 00 00 00 00 00 00
00405715 00 00 00 00 00 00 00 00
00405720 00 00 00 00 00 00 00 00
00405725 00 00 00 00 00 00 00 00
00405730 00 00 00 00 00 00 00 00
00405735 00 00 00 00 00 00 00 00
00405740 00 00 00 00 00 00 00 00
00405745 00 00 00 00 00 00 00 00
00405750 00 00 00 00 00 00 00 00
00405755 00 00 00 00 00 00 00 00
00405760 00 00 00 00 00 00 00 00
00405765 00 00 00 00 00 00 00 00
00405770 00 00 00 00 00 00 00 00
00405775 00 00 00 00 00 00 00 00
00405780 00 00 00 00 00 00 00 00
00405785 00 00 00 00 00 00 00 00
00405790 00 00 00 00 00 00 00 00
00405795 00 00 00 00 00 00 00 00
004057A0 00 00 00 00 00 00 00 00
004057A5 00 00 00 00 00 00 00 00
004057B0 00 00 00 00 00 00 00 00
004057B5 00 00 00 00 00 00 00 00
004057C0 00 00 00 00 00 00 00 00
004057C5 00 00 00 00 00 00 00 00
004057D0 00 00 00 00 00 00 00 00
004057D5 00 00 00 00 00 00 00 00
004057E0 00 00 00 00 00 00 00 00
004057E5 00 00 00 00 00 00 00 00
004057F0 00 00 00 00 00 00 00 00
004057F5 00 00 00 00 00 00 00 00
00405800 00 00 00 00 00 00 00 00
00405805 00 00 00 00 00 00 00 00
00405810 00 00 00 00 00 00 00 00
00405815 00 00 00 00 00 00 00 00
00405820 00 00 00 00 00 00 00 00
00405825 00 00 00 00 00 00 00 00
00405830 00 00 00 00 00 00 00 00
00405835 00 00 00 00 00 00 00 00
00405840 00 00 00 00 00 00 00 00
00405845 00 00 00 00 00 00 00 00
00405850 00 00 00 00 00 00 00 00
00405855 00 00 00 00 00 00 00 00
00405860 00 00 00 00 00 00 00 00
00405865 00 00 00 00 00 00 00 00
00405870 00 00 00 00 00 00 00 00
00405875 00 00 00 00 00 00 00 00
00405880 00 00 00 00 00 00 00 00
00405885 00 00 00 00 00 00 00 00
00405890 00 00 00 00 00 00 00 00
00405895 00 00 00 00 00 00 00 00
004058A0 00 00 00 00 00 00 00 00
004058A5 00 00 00 00 00 00 00 00
004058B0 00 00 00 00 00 00 00 00
004058B5 00 00 00 00 00 00 00 00
004058C0 00 00 00 00 00 00 00 00
004058C5 00 00 00 00 00 00 00 00
004058D0 00 00 00 00 00 00 00 00
004058D5 00 00 00 00 00 00 00 00
004058E0 00 00 00 00 00 00 00 00
004058E5 00 00 00 00 00 00 00 00
004058F0 00 00 00 00 00 00 00 00
004058F5 00 00 00 00 00 00 00 00
00405900 00 00 00 00 00 00 00 00
00405905 00 00 00 00 00 00 00 00
00405910 00 00 00 00 00 00 00 00
00405915 00 00 00 00 00 00 00 00
00405920 00 00 00 00 00 00 00 00
00405925 00 00 00 00 00 00 00 00
00405930 00 00 00 00 00 00 00 00
00405935 00 00 00 00 00 00 00 00
00405940 00 00 00 00 00 00 00 00
00405945 00 00 00 00 00 00 00 00
00405950 00 00 00 00 00 00 00 00
00405955 00 00 00 00 00 00 00 00
00405960 00 00 00 00 00 00 00 00
00405965 00 00 00 00 00 00 00 00
00405970 00 00 00 00 00 00 00 00<