

Soluzione - All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «Command Line» che viene passato sullo stack? Il valore del parametro è «CMD» ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo 00401067

00401057	8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	pStartupInfo
0040105A	50	PUSH EAX	CurrentDir = NULL
0040105B	6A 00	PUSH 0	pEnvironment = NULL
0040105D	6A 00	PUSH 0	CreationFlags = 0
0040105F	6A 00	PUSH 0	InheritHandles = TRUE
00401061	6A 01	PUSH 1	pThreadSecurity = NULL
00401063	6A 00	PUSH 0	pProcessSecurity = NULL
00401065	6A 00	PUSH 0	CommandLine = "cmd"
00401067	68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	6A 00	PUSH 0	CreateProcessA
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	Timeout = INFINITE
00401077	6A FF	PUSH -1	hObject
00401079	8B40 F0	MOV ECX,DWORD PTR SS:[EBP-10]	WaitForSingleObject
0040107C	51	PUSH ECX	
0040107D	FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSi	
00401083	33C0	XOR EAX,EAX	
00401085	8BE5	MOV ESP,EBP	
00401087	5D	POP EBP	
00401089	C2	RETN	

Soluzione – Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita? Una volta configurato il breakpoint, clicchiamo su «play», il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è «00000A28». Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà  
Prima

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 30404000	PUSH Malware_.004030C0	
00401586	64:R1 00000000	MOV EDX,DWORD PTR FS:[0]	
0040158C	59	PUSH EDI	
00401590	64:9225 000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	55	PUSH EBP	
00401598	8B5B	MOV EBX,EBP	
00401599	57	PUSH ESI	
0040159A	57	PUSH EDI	
0040159B	8B5B E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8044	MOV DL,AH	
004015A7	A915 D4524000	MOV DWORD PTR DS:[4052D41],FDX	

Dopo

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
00401579	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 30404000	PUSH Malware_.004030C0	
00401586	64:R1 00000000	MOV EDX,DWORD PTR FS:[0]	
0040158C	59	PUSH EDI	
00401590	64:9225 000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	55	PUSH EBP	
00401598	8B5B	MOV EBX,EBP	
00401599	57	PUSH ESI	
0040159A	57	PUSH EDI	
0040159B	8B5B E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8044	MOV DL,AH	
004015A7	A915 D4524000	MOV DWORD PTR DS:[4052D41],EDX	

Soluzione – Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita. Configuriamo il secondo breakpoint. Il valore del registro ECX è «0A280105».

Prima

The screenshot shows the OllyDbg interface with the assembly window displaying the following instructions:

```
00401577: 55      PUSH EBP
00401578: 68 FF   PUSH -1
00401579: 68 00404000 PUSH Malware_00404000
00401581: 68 3C204000 PUSH Malware_0040203C
00401586: 64:01 00000000 MOV EDI,DWORD PTR FS:[0]
0040158C: 59      PUSH EAX
00401590: 64:8925 00000000 MOV DWORD PTR FS:[0],ESP
00401594: 83EC 10  SUB ESP,10
00401597: 53      PUSH EBX
00401598: 56      PUSH ESI
00401599: 57      PUSH EDI
0040159A: 8965 E8  MOV DWORD PTR SS:[EBP-18],ESP
0040159B: FF15 30404000 CALL DWORD PTR DS:[<<KERNEL32.GetVersion
0040159D: 3302     XOR EDI,EDI
004015A0: 8A04     MOV DL,AH
004015A7: 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDI
004015AD: 8B08     MOV ECX,EAX
004015B0: 81E1 FF000000 AND ECX,0FF
004015B8: 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB: C1E1 08  SHL ECX,8
004015BE: 83C4     MOV ECX,EDX
004015C0: 8900 CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6: C1E8 10  SHR EDI,10
004015D0: 75 02     JNZ 004015D2
```

The Registers (FPU) window shows the following values:

Register	Value
EAX	00401577
ECX	00000005
EDX	00000001
EBX	77F04000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015AF Malware_004015AF
CS	001B 32bit 0FFFFFFF
DS	001B 32bit 0FFFFFFF
SS	0023 32bit 0FFFFFFF
ES	0023 32bit 0FFFFFFF
FS	0038 32bit 77F04000
GS	0000 NULL
IOPL	0
LastErr	ERROR_INVALID_HANDLE (00000000)
EFL	00000246 (NO, NB, E, BE, ST0 empty, UNORM BCBC 011, ST1 empty, UNORM 0069 80, ST2 empty, 0,0)

dopo lo step-into il valore del registro ECX è stato modificato in «00000005» in quanto è stata eseguita l'istruzione AND ECX, FF

Dopo

The screenshot shows the OllyDbg interface with the assembly window displaying the following instructions:

```
00401577: 55      PUSH EBP
00401578: 68 FF   PUSH -1
00401579: 68 00404000 PUSH Malware_00404000
00401581: 68 3C204000 PUSH Malware_0040203C
00401586: 64:01 00000000 MOV EDI,DWORD PTR FS:[0]
0040158C: 59      PUSH EAX
00401590: 64:8925 00000000 MOV DWORD PTR FS:[0],ESP
00401594: 83EC 10  SUB ESP,10
00401597: 53      PUSH EBX
00401598: 56      PUSH ESI
00401599: 57      PUSH EDI
0040159A: 8965 E8  MOV DWORD PTR SS:[EBP-18],ESP
0040159B: FF15 30404000 CALL DWORD PTR DS:[<<KERNEL32.GetVersion
0040159D: 3302     XOR EDI,EDI
004015A0: 8A04     MOV DL,AH
004015A7: 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDI
004015AD: 8B08     MOV ECX,EAX
004015B0: 81E1 FF000000 AND ECX,0FF
004015B8: 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB: C1E1 08  SHL ECX,8
004015BE: 83C4     MOV ECX,EDX
004015C0: 8900 CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6: C1E8 10  SHR EDI,10
004015D0: 75 02     JNZ 004015D2
004015D2: 74 02     JZ 004015D4
004015D4: 75 02     JNZ 004015D6
004015D6: 74 02     JZ 004015D8
004015D8: 75 02     JNZ 004015DA
004015DA: 74 02     JZ 004015DC
004015DC: 75 02     JNZ 004015DE
004015DE: 74 02     JZ 004015E0
004015E0: 75 02     JNZ 004015E2
004015E2: 74 02     JZ 004015E4
004015E4: 75 02     JNZ 004015E6
004015E6: 74 02     JZ 004015E8
004015E8: 75 02     JNZ 004015EA
004015EA: 74 02     JZ 004015EC
004015EC: 75 02     JNZ 004015EE
004015EE: 74 02     JZ 004015F0
004015F0: 75 02     JNZ 004015F2
004015F2: 74 02     JZ 004015F4
004015F4: 75 02     JNZ 004015F6
004015F6: 74 02     JZ 004015F8
004015F8: 75 02     JNZ 004015FA
004015FA: 74 02     JZ 004015FC
004015FC: 75 02     JNZ 004015FE
004015FE: 74 02     JZ 00401600
00401600: 75 02     JNZ 00401602
00401602: 74 02     JZ 00401604
00401604: 75 02     JNZ 00401606
00401606: 74 02     JZ 00401608
00401608: 75 02     JNZ 0040160A
0040160A: 74 02     JZ 0040160C
0040160C: 75 02     JNZ 0040160E
0040160E: 74 02     JZ 00401610
00401610: 75 02     JNZ 00401612
00401612: 74 02     JZ 00401614
00401614: 75 02     JNZ 00401616
00401616: 74 02     JZ 00401618
00401618: 75 02     JNZ 0040161A
0040161A: 74 02     JZ 0040161C
0040161C: 75 02     JNZ 0040161E
0040161E: 74 02     JZ 00401620
00401620: 75 02     JNZ 00401622
00401622: 74 02     JZ 00401624
00401624: 75 02     JNZ 00401626
00401626: 74 02     JZ 00401628
00401628: 75 02     JNZ 0040162A
0040162A: 74 02     JZ 0040162C
0040162C: 75 02     JNZ 0040162E
0040162E: 74 02     JZ 00401630
00401630: 75 02     JNZ 00401632
00401632: 74 02     JZ 00401634
00401634: 75 02     JNZ 00401636
00401636: 74 02     JZ 00401638
00401638: 75 02     JNZ 0040163A
0040163A: 74 02     JZ 0040163C
0040163C: 75 02     JNZ 0040163E
0040163E: 74 02     JZ 00401640
00401640: 75 02     JNZ 00401642
00401642: 74 02     JZ 00401644
00401644: 75 02     JNZ 00401646
00401646: 74 02     JZ 00401648
00401648: 75 02     JNZ 0040164A
0040164A: 74 02     JZ 0040164C
0040164C: 75 02     JNZ 0040164E
0040164E: 74 02     JZ 00401650
00401650: 75 02     JNZ 00401652
00401652: 74 02     JZ 00401654
00401654: 75 02     JNZ 00401656
00401656: 74 02     JZ 00401658
00401658: 75 02     JNZ 0040165A
0040165A: 74 02     JZ 0040165C
0040165C: 75 02     JNZ 0040165E
0040165E: 74 02     JZ 00401660
00401660: 75 02     JNZ 00401662
00401662: 74 02     JZ 00401664
00401664: 75 02     JNZ 00401666
00401666: 74 02     JZ 00401668
00401668: 75 02     JNZ 0040166A
0040166A: 74 02     JZ 0040166C
0040166C: 75 02     JNZ 0040166E
0040166E: 74 02     JZ 00401670
00401670: 75 02     JNZ 00401672
00401672: 74 02     JZ 00401674
00401674: 75 02     JNZ 00401676
00401676: 74 02     JZ 00401678
00401678: 75 02     JNZ 0040167A
0040167A: 74 02     JZ 0040167C
0040167C: 75 02     JNZ 0040167E
0040167E: 74 02     JZ 00401680
00401680: 75 02     JNZ 00401682
00401682: 74 02     JZ 00401684
00401684: 75 02     JNZ 00401686
00401686: 74 02     JZ 00401688
00401688: 75 02     JNZ 0040168A
0040168A: 74 02     JZ 0040168C
0040168C: 75 02     JNZ 0040168E
0040168E: 74 02     JZ 00401690
00401690: 75 02     JNZ 00401692
00401692: 74 02     JZ 00401694
00401694: 75 02     JNZ 00401696
00401696: 74 02     JZ 00401698
00401698: 75 02     JNZ 0040169A
0040169A: 74 02     JZ 0040169C
0040169C: 75 02     JNZ 0040169E
0040169E: 74 02     JZ 004016A0
004016A0: 75 02     JNZ 004016A2
004016A2: 74 02     JZ 004016A4
004016A4: 75 02     JNZ 004016A6
004016A6: 74 02     JZ 004016A8
004016A8: 75 02     JNZ 004016AA
004016AA: 74 02     JZ 004016AC
004016AC: 75 02     JNZ 004016AE
004016AE: 74 02     JZ 004016B0
004016B0: 75 02     JNZ 004016B2
004016B2: 74 02     JZ 004016B4
004016B4: 75 02     JNZ 004016B6
004016B6: 74 02     JZ 004016B8
004016B8: 75 02     JNZ 004016BA
004016BA: 74 02     JZ 004016BC
004016BC: 75 02     JNZ 004016BE
004016BE: 74 02     JZ 004016C0
004016C0: 75 02     JNZ 004016C2
004016C2: 74 02     JZ 004016C4
004016C4: 75 02     JNZ 004016C6
004016C6: 74 02     JZ 004016C8
004016C8: 75 02     JNZ 004016CA
004016CA: 74 02     JZ 004016CC
004016CC: 75 02     JNZ 004016CE
004016CE: 74 02     JZ 004016D0
004016D0: 75 02     JNZ 004016D2
004016D2: 74 02     JZ 004016D4
004016D4: 75 02     JNZ 004016D6
004016D6: 74 02     JZ 004016D8
004016D8: 75 02     JNZ 004016DA
004016DA: 74 02     JZ 004016DC
004016DC: 75 02     JNZ 004016DE
004016DE: 74 02     JZ 004016E0
004016E0: 75 02     JNZ 004016E2
004016E2: 74 02     JZ 004016E4
004016E4: 75 02     JNZ 004016E6
004016E6: 74 02     JZ 004016E8
004016E8: 75 02     JNZ 004016EA
004016EA: 74 02     JZ 004016EC
004016EC: 75 02     JNZ 004016EE
004016EE: 74 02     JZ 004016F0
004016F0: 75 02     JNZ 004016F2
004016F2: 74 02     JZ 004016F4
004016F4: 75 02     JNZ 004016F6
004016F6: 74 02     JZ 004016F8
004016F8: 75 02     JNZ 004016FA
004016FA: 74 02     JZ 004016FC
004016FC: 75 02     JNZ 004016FE
004016FE: 74 02     JZ 00401700
00401700: 75 02     JNZ 00401702
00401702: 74 02     JZ 00401704
00401704: 75 02     JNZ 00401706
00401706: 74 02     JZ 00401708
00401708: 75 02     JNZ 0040170A
0040170A: 74 02     JZ 0040170C
0040170C: 75 02     JNZ 0040170E
0040170E: 74 02     JZ 00401710
00401710: 75 02     JNZ 00401712
00401712: 74 02     JZ 00401714
00401714: 75 02     JNZ 00401716
00401716: 74 02     JZ 00401718
00401718: 75 02     JNZ 0040171A
0040171A: 74 02     JZ 0040171C
0040171C: 75 02     JNZ 0040171E
0040171E: 74 02     JZ 00401720
00401720: 75 02     JNZ 00401722
00401722: 74 02     JZ 00401724
00401724: 75 02     JNZ 00401726
00401726: 74 02     JZ 00401728
00401728: 75 02     JNZ 0040172A
0040172A: 74 02     JZ 0040172C
0040172C: 75 02     JNZ 0040172E
0040172E: 74 02     JZ 00401730
00401730: 75 02     JNZ 00401732
00401732: 74 02     JZ 00401734
00401734: 75 02     JNZ 00401736
00401736: 74 02     JZ 00401738
00401738: 75 02     JNZ 0040173A
0040173A: 74 02     JZ 0040173C
0040173C: 75 02     JNZ 0040173E
0040173E: 74 02     JZ 00401740
00401740: 75 02     JNZ 00401742
00401742: 74 02     JZ 00401744
00401744: 75 02     JNZ 00401746
00401746: 74 02     JZ 00401748
00401748: 75 02     JNZ 0040174A
0040174A: 74 02     JZ 0040174C
0040174C: 75 02     JNZ 0040174E
0040174E: 74 02     JZ 00401750
00401750: 75 02     JNZ 00401752
00401752: 74 02     JZ 00401754
00401754: 75 02     JNZ 00401756
00401756: 74 02     JZ 00401758
00401758: 75 02     JNZ 0040175A
0040175A: 74 02     JZ 0040175C
0040175C: 75 02     JNZ 0040175E
0040175E: 74 02     JZ 00401760
00401760: 75 02     JNZ 00401762
00401762: 74 02     JZ 00401764
00401764: 75 02     JNZ 00401766
00401766: 74 02     JZ 00401768
00401768: 75 02     JNZ 0040176A
0040176A: 74 02     JZ 0040176C
0040176C: 75 02     JNZ 0040176E
0040176E: 74 02     JZ 00401770
00401770: 75 02     JNZ 00401772
00401772: 74 02     JZ 00401774
00401774: 75 02     JNZ 00401776
00401776: 74 02     JZ 00401778
00401778: 75 02     JNZ 0040177A
0040177A: 74 02     JZ 0040177C
0040177C: 75 02     JNZ 0040177E
0040177E: 74 02     JZ 00401780
00401780: 75 02     JNZ 00401782
00401782: 74 02     JZ 00401784
00401784: 75 02     JNZ 00401786
00401786: 74 02     JZ 00401788
00401788: 75 02     JNZ 0040178A
0040178A: 74 02     JZ 0040178C
0040178C: 75 02     JNZ 0040178E
0040178E: 74 02     JZ 00401790
00401790: 75 02     JNZ 00401792
00401792: 74 02     JZ 00401794
00401794: 75 02     JNZ 00401796
00401796: 74 02     JZ 00401798
00401798: 75 02     JNZ 0040179A
0040179A: 74 02     JZ 0040179C
0040179C: 75 02     JNZ 0040179E
0040179E: 74 02     JZ 004017A0
004017A0: 75 02     JNZ 004017A2
004017A2: 74 02     JZ 004017A4
004017A4: 75 02     JNZ 004017A6
004017A6: 74 02     JZ 004017A8
004017A8: 75 02     JNZ 004017AA
004017AA: 74 02     JZ 004017AC
004017AC: 75 02     JNZ 004017AE
004017AE: 74 02     JZ 004017B0
004017B0: 75 02     JNZ 004017B2
004017B2: 74 02     JZ 004017B4
004017B4: 75 02     JNZ 004017B6
004017B6: 74 02     JZ 004017B8
004017B8: 75 02     JNZ 004017BA
004017BA: 74 02     JZ 004017BC
004017BC: 75 02     JNZ 004017BE
004017BE: 74 02     JZ 004017C0
004017C0: 75 02     JNZ 004017C2
004017C2: 74 02     JZ 004017C4
004017C4: 75 02     JNZ 004017C6
004017C6: 74 02     JZ 004017C8
004017C8: 75 02     JNZ 004017CA
004017CA: 74 02     JZ 004017CC
004017CC: 75 02     JNZ 004017CE
004017CE: 74 02     JZ 004017D0
004017D0: 75 02     JNZ 004017D2
004017D2: 74 02     JZ 004017D4
004017D4: 75 02     JNZ 004017D6
004017D6: 74 02     JZ 004017D8
004017D8: 75 02     JNZ 004017DA
004017DA: 74 02     JZ 004017DC
004017DC: 75 02     JNZ 004017DE
004017DE: 74 02     JZ 004017E0
004017E0: 75 02     JNZ 004017E2
004017E2: 74 02     JZ 004017E4
004017E4: 75 02     JNZ 004017E6
004017E6: 74 02     JZ 004017E8
004017E8: 75 02     JNZ 004017EA
004017EA: 74 02     JZ 004017EC
004017EC: 75 02     JNZ 004017EE
004017EE: 74 02     JZ 004017F0
004017F0: 75 02     JNZ 004017F2
004017F2: 74 02     JZ 004017F4
004017F4: 75 02     JNZ 004017F6
004017F6: 74 02     JZ 004017F8
004017F8: 75 02     JNZ 004017FA
004017FA: 74 02     JZ 004017FC
004017FC: 75 02     JNZ 004017FE
004017FE: 74 02     JZ 00401800
00401800: 75 02     JNZ 00401802
00401802: 74 02     JZ 00401804
00401804: 75 02     JNZ 00401806
00401806: 74 02     JZ 00401808
00401808: 75 02     JNZ 0040180A
0040180A: 74 02     JZ 0040180C
0040180C: 75 02     JNZ 0040180E
0040180E: 74 02     JZ 00401810
00401810: 75 02     JNZ 00401812
00401812: 74 02     JZ 00401814
00401814: 75 02     JNZ 00401816
00401816: 74 02     JZ 00401818
00401818: 75 02     JNZ 0040181A
0040181A: 74 02     JZ 0040181C
0040181C: 75 02     JNZ 0040181E
0040181E: 74 02     JZ 00401820
00401820: 75 02     JNZ 00401822
00401822: 74 02     JZ 00401824
00401824: 75 02     JNZ 00401826
00401826: 74 02     JZ 00401828
00401828: 75 02     JNZ 0040182A
0040182A: 74 02     JZ 0040182C
0040182C: 75 02     JNZ 0040182E
0040182E: 74 02     JZ 00401830
00401830: 75 02     JNZ 00401832
00401832: 74 02     JZ 00401834
00401834: 75 02     JNZ 00401836
00401836: 74 02     JZ 00401838
00401838: 75 02     JNZ 0040183A
0040183A: 74 02     JZ 0040183C
0040183C: 75 02     JNZ 0040183E
0040183E: 74 02     JZ 00401840
00401840: 75 02     JNZ 00401842
00401842: 74 02     JZ 00401844
00401844: 75 02     JNZ 00401846
00401846: 74 02     JZ 00401848
00401848: 75 02     JNZ 0040184A
0040184A: 74 02     JZ 0040184C
0040184C: 75 02     JNZ 0040184E
0040184E: 74 02     JZ 00401850
00401850: 75 02     JNZ 00401852
00401852: 74 02     JZ 00401854
00401854: 75 02     JNZ 00401856
00401856: 74 02     JZ 00401858
00401858: 75 02     JNZ 0040185A
0040185A: 74 02     JZ 0040185C
0040185C: 75 02     JNZ 0040185E
0040185E: 74 02     JZ 00401860
00401860: 75 02     JNZ 00401862
00401862: 74 02     JZ 00401864
00401864: 75 02     JNZ 00401866
00401866: 74 02     JZ 00401868
00401868: 75 02     JNZ 0040186A
0040186A: 74 02     JZ 0040186C
0040186C: 75 02     JNZ 0040186E
0040186E: 74 02     JZ 00401870
00401870: 75 02     JNZ 00401872
00401872: 74 02     JZ 00401874
00401874: 75 02     JNZ 00401876
00401876: 74 02     JZ 00401878
00401878: 75 02     JNZ 0040187A
0040187A: 74 02     JZ 0040187C
0040187C: 75 02     JNZ 0040187E
0040187E: 74 02     JZ 00401880
00401880: 75 02     JNZ 00401882
00401882: 74 02     JZ 00401884
00401884: 75 02     JNZ 00401886
00401886: 74 02     JZ 00401888
00401888: 75 02     JNZ 0040188A
0040188A: 74 02     JZ 0040188C
0040188C: 75 02     JNZ 0040188E
0040188E: 74 02     JZ 00401890
00401890: 75 02     JNZ 00401892
00401892: 74 02     JZ 00401894
00401894: 75 02     JNZ 00401896
00401896: 74 02     JZ 00401898
00401898: 75 02     JNZ 0040189A
0040189A: 74 02     JZ 0040189C
0040189C: 75 02     JNZ 0040189E
0040189E: 74 02     JZ 004018A0
004018A0: 75 02     JNZ 004018A2
004018A2: 74 02     JZ 004018A4
004018A4: 75 02     JNZ 004018A6
004018A6: 74 02     JZ 004018A8
004018A8: 75 02     JNZ 004018AA
004018AA: 74 02     JZ 004018AC
004018AC: 75 02     JNZ 004018AE
004018AE: 74 02     JZ 004018B0
004018B0: 75 02     JNZ 004018B2
004018B2: 74 02     JZ 004018B4
004018B4: 75 02     JNZ 004018B6
004018B6: 74 02     JZ 004018B8
004018B8: 75 02
```