

1

0012FE5C	7C90DE5C	RETURN to ntdll.7C90DE5C
0012FE60	7C81CAB6	RETURN to kernel32.7C81CAB6
0012FE64	FFFFFFFF	
0012FE68	00000001	
0012FE6C	00000001	
0012FE70	FFFFFFFF	
0012FE74	7FFDB000	
0012FE78	00000000	
0012FE7C	00300014	
0012FE80	00000002	
0012FE84	00000580	
0012FE88	000004FC	
0012FE8C	0000C254	
0012FE90	00000000	
0012FE94	00000000	
0012FE98	00010003	
0012FE9C	00000000	
0012FEA0	7B7A7978	
0012FEA4	00000001	
0012FEA8	7C912CAE	RETURN to ntdll.7C912CAE from ntdll.RtlEnterCriticalSection
0012FEAC	7C912CE4	RETURN to ntdll.7C912CE4 from ntdll.7C90E8E6
0012FEB0	7C912D51	RETURN to ntdll.7C912D51 from ntdll.RtlLeaveCriticalSection
0012FEB4	7C912D58	RETURN to ntdll.7C912D58 from ntdll.7C90E8E6
0012FEB8	00000006	
0012FEBC	00241EE0	
0012FEC0	00000208	
0012FEC4	9F9E9D9C	
0012FEC8	0012FEB8	
0012FEC C	A7A6A5A4	
0012FED0	0012FF28	
0012FED4	00000000	
0012FED8	00000000	
0012FEDC	FFFFFFFF	

Il valore del parametro *CommandLine* è memorizzato nella memoria dello stack all'indirizzo *0x0012FE5C*. Questo valore è una stringa di 14 caratteri che rappresenta un messaggio che viene visualizzato quando il codice viene eseguito in modo anomalo.

2

Registers (FPU)	
EAX	0A280105
ECX	7FFD6000
EDX	00000A28
EBX	7FFD6000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015A3 Malware_.004015A3
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastError ERROR_INVALID_HANDLE (00000006)
EFL	00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0	empty -UNORM BCBC 01050104 0054005C
ST1	empty +UNORM 0061 0072006F 0070006D
ST2	empty +UNORM 0063 00650072 00690044
ST3	empty +UNORM 0066 00200034 00200079
ST4	empty +UNORM 0073 006E0061 00720074
ST5	empty +UNORM 006F 006C0063 0070002E
ST6	empty +UNORM 0062 0073006A 004C0070
ST7	empty +UNORM 005C 00700069 007A002E
3 2 1 0 E S P U O Z D I	
FST 0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)
FCW 027F	Prec NEAR,53 Mask 1 1 1 1 1 1

Il valore del registro EDX è *00000A28*.

3 - 4 - 5

0040155F	F7D9	NEG ECX			
00401561	4F	DEC EDI			
00401562	8A45 0C	MOV AL, BYTE PTR SS:[EBP+C]			
00401565	FD	STD			
00401566	F2:AE	REPNE SCAS BYTE PTR ES:[EDI]			
00401569	47	INC EDI			
00401569	8007	CMPL BYTE PTR DS:[EDI], AL			
0040156B	74 04	JE SHORT Malware_.00401571			
0040156D	38C0	XOR ECX, ECX			
0040156F	EB 02	JMP SHORT Malware_.00401573			
00401571	8BC7	MOV EAX, EDI			
00401573	F0	CJLE			
00401574	5F	POP EDI			
00401575	C9	LEAVE			
00401576	C3	RET			
00401577	55	PUSH ESP			
00401578	8BEC	MOV EBP, ESP			
0040157A	6A FF	PUSH -1			
0040157C	68 00404000	PUSH Malware_.00404000			
00401581	68 3C204000	PUSH Malware_.0040203C			
00401586	64:A1 00000000	MOV EAX, DWORD PTR FS:[0]	SE handler installation		
0040158C	50	PUSH ECX			
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0], ESP			
00401594	8BEC 10	SUB ESP, 10			
00401597	53	PUSH EBX			
00401598	56	PUSH ESI			
00401599	57	PUSH EDI			
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-10], ESP			
0040159A	FF15 30404000	CALL DWORD PTR DS:[<KERNEL32.GetVersion	kernel32.GetVersion		
0040159B	30C0	XOR EDX, EDX			
0040159B	8004	MOV DL, AH			
00401597	8915 04524000	MOV DWORD PTR DS:[4052D4], EDX			
004015A0	8BC3	MOV ECX, ECX			
004015AF	81E1 FF000000	AND ECX, 0			
004015B5	8900 00524000	MOV DWORD PTR DS:[4052D0], ECX			
004015B8	C1E1 08	SHL ECX, 8			
004015BE	03CA	ADD ECX, EDX			
004015C0	8900 CC524000	MOV DWORD PTR DS:[4052CC], ECX			
004015C6	C1E8 10	SHR ECX, 10			
004015C9	A3 CC524000	MOV DWORD PTR DS:[4052C8], ECX			
004015CE	6A 00	PUSH 0			
004015D0	E8 33090000	CALL Malware_.00401F08			
004015D5	59	POP ECX			
004015D6	85C0	TEST EAX, EAX			
004015D9	75 08	JNZ SHORT Malware_.004015E2			
004015DA	6A 1C	PUSH 1C			
004015DC	E8 9A000000	CALL Malware_.00401678			
004015E1	59	POP ECX			
004015E2	8965 FC 00	MOV DWORD PTR SS:[EBP-4], 0			
004015E5	E8 72070000	CALL Malware_.00401D5D			
004015EB	FF15 2C404000	CALL DWORD PTR DS:[<KERNEL32.GetCommandL	CGetCommandLineA		
004015F1	A3 08574000	MOV DWORD PTR DS:[4057D0], EAX			
004015F6	E8 30060000	CALL Malware_.00401C28			
004015FB	A3 80524000	MOV DWORD PTR DS:[4052B0], EAX			
00401600	E8 19030000	CALL Malware_.0040150E			
00401605	E8 1B030000	CALL Malware_.0040150E			
0040160A	E8 90000000	CALL Malware_.0040169F			

Registers (FPU)			
EAX	00000000	ECX	7FFD6000
EDX	00000000	EBX	7FFD6000
ESP	0012FF94	EBP	0012FFC0
ESI	FFFFFFFF	EDI	7C910208 ntdll.7C910208
EIP	00401595	Malware_.00401595	
C 0	ES 0023 32bit 0(FFFFFFFF)	P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)	Z 1	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)	T 0	GS 0000 NULL
D 0			
O 0	LastErr ERROR_INVALID_HANDLE (00000006)		
EPL	00010246 (NO, NB, E, BE, MS, FE, GE, LE)		
ST0	empty -UNORM DCBC 01950104 0054005C	ST1	empty -UNORM 0061 0072006F 0070006D
ST2	empty -UNORM 0063 00650072 00690044	ST3	empty -UNORM 0066 00680034 00600079
ST4	empty -UNORM 0073 006E0061 00720074	ST5	empty -UNORM 006F 006C0063 0070005E
ST6	empty -UNORM 0062 00730064 004C0070	ST7	empty -UNORM 005C 00700069 0070003E
FST	0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (6T)		
FCW	027F Prec NEAR, SS Mask 1 1 1 1 1 1		

Dopo aver eseguito uno *step-into* dal *breakpoint* impostato, il valore del registro *EDX* è ora 0. Questo perché il breakpoint è stato impostato sulla linea di codice che inizializza il registro *EDX* a 0. L'istruzione che è stata eseguita è

mov edx, 0

Essa sposta il valore 0 nel registro *EDX*. Quando si esegue uno *step-into*, il *debugger* passa alla successiva istruzione di codice. In questo caso, l'istruzione successiva è quella che ho appena messo in evidenza. Pertanto, il valore del registro *EDX* è ora 0.

The screenshot shows a debugger window with the following components:

- Assembly View:** Displays assembly instructions with their addresses and hex values. The instruction at address 004015AF is highlighted in red.


```

      004015AF 8B45 0C      MOV     ECX, [EBP+0C]
      004015B0 8B45 0C      MOV     ECX, [EBP+0C]
      004015B1 8B45 0C      MOV     ECX, [EBP+0C]
      004015B2 8B45 0C      MOV     ECX, [EBP+0C]
      004015B3 8B45 0C      MOV     ECX, [EBP+0C]
      004015B4 8B45 0C      MOV     ECX, [EBP+0C]
      004015B5 8B45 0C      MOV     ECX, [EBP+0C]
      004015B6 8B45 0C      MOV     ECX, [EBP+0C]
      004015B7 8B45 0C      MOV     ECX, [EBP+0C]
      004015B8 8B45 0C      MOV     ECX, [EBP+0C]
      004015B9 8B45 0C      MOV     ECX, [EBP+0C]
      004015BA 8B45 0C      MOV     ECX, [EBP+0C]
      004015BB 8B45 0C      MOV     ECX, [EBP+0C]
      004015BC 8B45 0C      MOV     ECX, [EBP+0C]
      004015BD 8B45 0C      MOV     ECX, [EBP+0C]
      004015BE 8B45 0C      MOV     ECX, [EBP+0C]
      004015BF 8B45 0C      MOV     ECX, [EBP+0C]
      004015C0 8B45 0C      MOV     ECX, [EBP+0C]
      004015C1 8B45 0C      MOV     ECX, [EBP+0C]
      004015C2 8B45 0C      MOV     ECX, [EBP+0C]
      004015C3 8B45 0C      MOV     ECX, [EBP+0C]
      004015C4 8B45 0C      MOV     ECX, [EBP+0C]
      004015C5 8B45 0C      MOV     ECX, [EBP+0C]
      004015C6 8B45 0C      MOV     ECX, [EBP+0C]
      004015C7 8B45 0C      MOV     ECX, [EBP+0C]
      004015C8 8B45 0C      MOV     ECX, [EBP+0C]
      004015C9 8B45 0C      MOV     ECX, [EBP+0C]
      004015CA 8B45 0C      MOV     ECX, [EBP+0C]
      004015CB 8B45 0C      MOV     ECX, [EBP+0C]
      004015CC 8B45 0C      MOV     ECX, [EBP+0C]
      004015CD 8B45 0C      MOV     ECX, [EBP+0C]
      004015CE 8B45 0C      MOV     ECX, [EBP+0C]
      004015CF 8B45 0C      MOV     ECX, [EBP+0C]
      004015D0 8B45 0C      MOV     ECX, [EBP+0C]
      004015D1 8B45 0C      MOV     ECX, [EBP+0C]
      004015D2 8B45 0C      MOV     ECX, [EBP+0C]
      004015D3 8B45 0C      MOV     ECX, [EBP+0C]
      004015D4 8B45 0C      MOV     ECX, [EBP+0C]
      004015D5 8B45 0C      MOV     ECX, [EBP+0C]
      004015D6 8B45 0C      MOV     ECX, [EBP+0C]
      004015D7 8B45 0C      MOV     ECX, [EBP+0C]
      004015D8 8B45 0C      MOV     ECX, [EBP+0C]
      004015D9 8B45 0C      MOV     ECX, [EBP+0C]
      004015DA 8B45 0C      MOV     ECX, [EBP+0C]
      004015DB 8B45 0C      MOV     ECX, [EBP+0C]
      004015DC 8B45 0C      MOV     ECX, [EBP+0C]
      004015DD 8B45 0C      MOV     ECX, [EBP+0C]
      004015DE 8B45 0C      MOV     ECX, [EBP+0C]
      004015DF 8B45 0C      MOV     ECX, [EBP+0C]
      004015E0 8B45 0C      MOV     ECX, [EBP+0C]
      004015E1 8B45 0C      MOV     ECX, [EBP+0C]
      004015E2 8B45 0C      MOV     ECX, [EBP+0C]
      004015E3 8B45 0C      MOV     ECX, [EBP+0C]
      004015E4 8B45 0C      MOV     ECX, [EBP+0C]
      004015E5 8B45 0C      MOV     ECX, [EBP+0C]
      004015E6 8B45 0C      MOV     ECX, [EBP+0C]
      004015E7 8B45 0C      MOV     ECX, [EBP+0C]
      004015E8 8B45 0C      MOV     ECX, [EBP+0C]
      004015E9 8B45 0C      MOV     ECX, [EBP+0C]
      004015EA 8B45 0C      MOV     ECX, [EBP+0C]
      004015EB 8B45 0C      MOV     ECX, [EBP+0C]
      004015EC 8B45 0C      MOV     ECX, [EBP+0C]
      004015ED 8B45 0C      MOV     ECX, [EBP+0C]
      004015EE 8B45 0C      MOV     ECX, [EBP+0C]
      004015EF 8B45 0C      MOV     ECX, [EBP+0C]
      004015F0 8B45 0C      MOV     ECX, [EBP+0C]
      004015F1 8B45 0C      MOV     ECX, [EBP+0C]
      004015F2 8B45 0C      MOV     ECX, [EBP+0C]
      004015F3 8B45 0C      MOV     ECX, [EBP+0C]
      004015F4 8B45 0C      MOV     ECX, [EBP+0C]
      004015F5 8B45 0C      MOV     ECX, [EBP+0C]
      004015F6 8B45 0C      MOV     ECX, [EBP+0C]
      004015F7 8B45 0C      MOV     ECX, [EBP+0C]
      004015F8 8B45 0C      MOV     ECX, [EBP+0C]
      004015F9 8B45 0C      MOV     ECX, [EBP+0C]
      004015FA 8B45 0C      MOV     ECX, [EBP+0C]
      004015FB 8B45 0C      MOV     ECX, [EBP+0C]
      004015FC 8B45 0C      MOV     ECX, [EBP+0C]
      004015FD 8B45 0C      MOV     ECX, [EBP+0C]
      004015FE 8B45 0C      MOV     ECX, [EBP+0C]
      004015FF 8B45 0C      MOV     ECX, [EBP+0C]
      
```
- Registers (FPU):** Shows the current values of the registers. The ECX register is highlighted in red.


```

      EAX 00200105
      ECX 7FFD6000
      EDI 00000000
      ESI 7FFD6000
      ESP 0012FF94
      EBP 0012FF94
      EIP 004015AF Malware_.004015AF
      
```
- Comments:** The instruction at 004015AF is annotated with "SE handler installation" and "kernel32.GetVersion".

Dopo aver impostato un secondo *breakpoint* all'indirizzo di memoria 004015AF, il valore del registro *ECX* è 7FFD6000.

MOV DWORD PTR DS:[4052D4],EDX

Bonus

Potrebbe essere un ransomware, ma non ne sono sicuro.