

Malware Analysis

OllyDBG

Cyber Security & Ethical

1

All'indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» 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

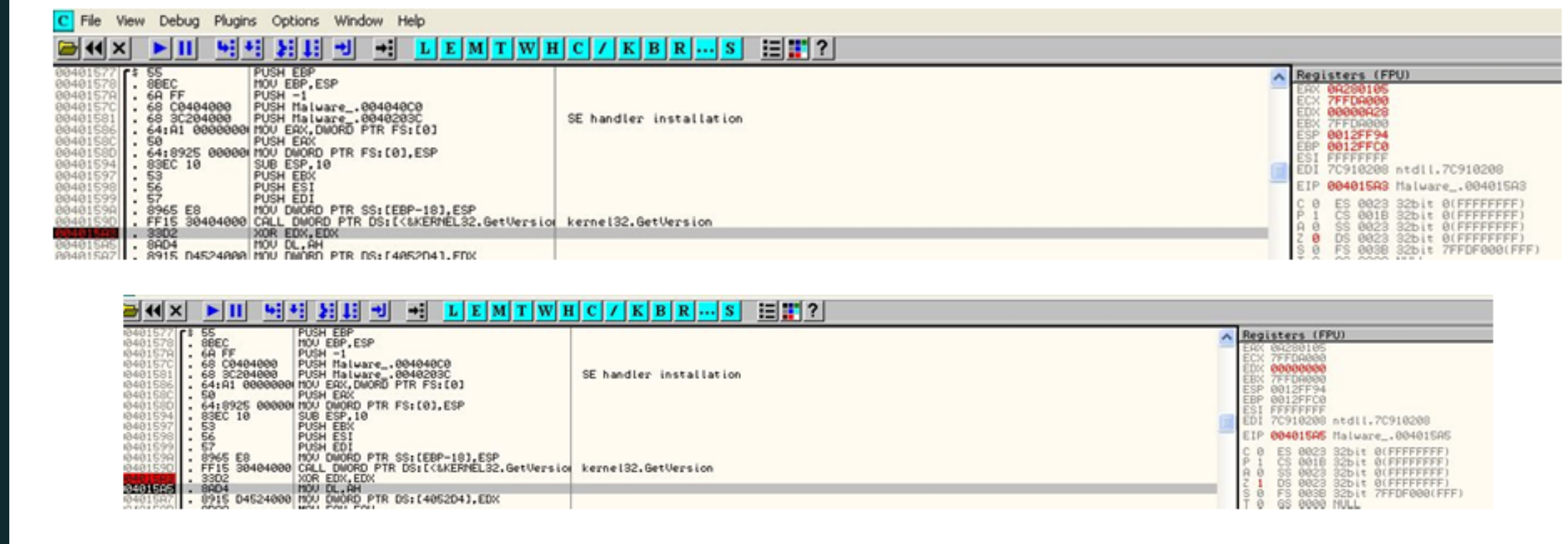
Address	Disassembly	Comment
00401057	8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]
0040105A	50	PUSH EAX
0040105B	6A 00	PUSH 0
0040105D	6A 00	PUSH 0
0040105F	6A 00	PUSH 0
00401061	6A 01	PUSH 1
00401063	6A 00	PUSH 0
00401065	6A 00	PUSH 0
00401067	68 30504000	PUSH Malware_.00405030
0040106C	6A 00	PUSH 0
0040106E	FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX
00401077	6A FF	PUSH -1
00401079	8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]
0040107C	51	PUSH ECX
0040107D	FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSingleObject]
00401083	33C0	XOR EAX,EAX
00401085	8BE5	MOV ESP,EBP
00401087	5D	POP EBP
00401089	C2	RETN

Parameter	Value
pStartupInfo	
CurrentDir	= NULL
pEnvironment	= NULL
CreationFlags	= 0
InheritHandles	= TRUE
pThreadSecurity	= NULL
pProcessSecurity	= NULL
CommandLine	= "cmd"
ModuleFileName	= NULL

2

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 0.

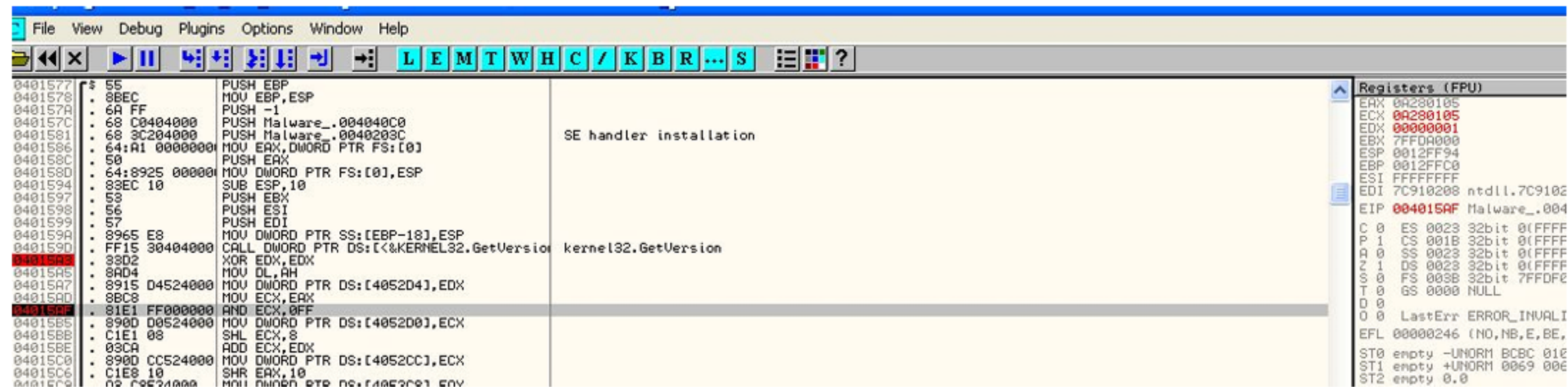


3

Inserezite 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 .

Configurando il secondo breakpoint. Il valore il valore del registro ECX è «0A280105»

PRIMA



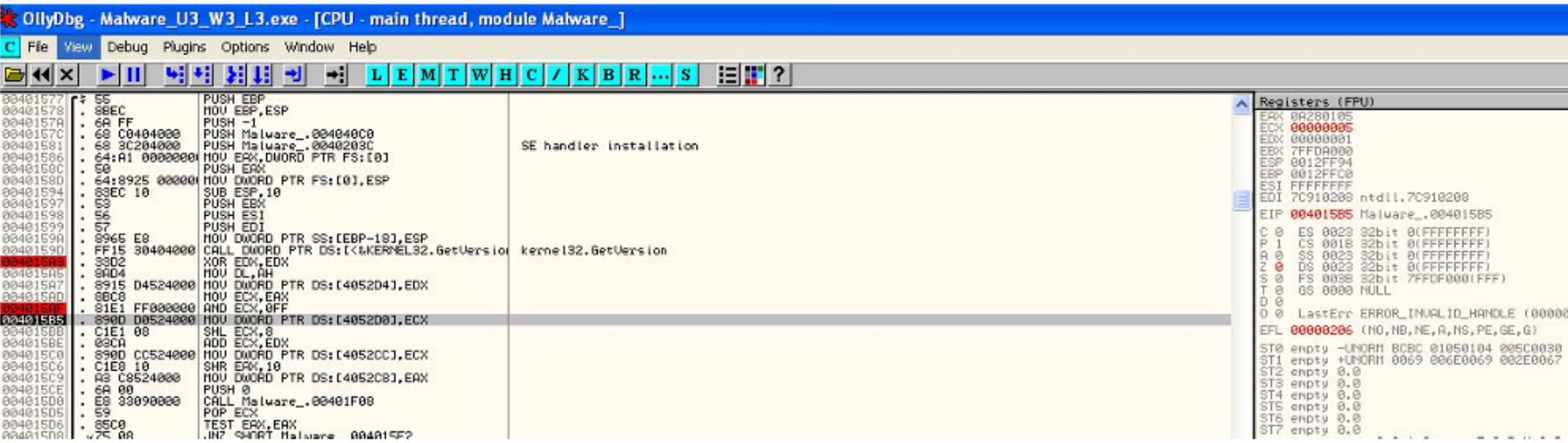
The screenshot shows a debugger window with the following components:

- Assembly List:** A list of assembly instructions with their addresses. The instruction at address 004015AF is highlighted in red. It is `AND ECX, 0FF`.
- Registers (FPU):** A panel on the right showing the current values of the registers. The ECX register is highlighted in red and shows the value `0A280105`.
- Disassembly:** A column on the right showing the disassembly of the instructions. The instruction at 004015AF is `AND ECX, 0FF`.
- Comments:** A column on the right showing comments for the instructions. The comment for the instruction at 004015AF is `kernel32.GetVersion`.

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV EBP, ESP	
00401579	PUSH -1	
0040157C	PUSH Malware_.004040C0	
00401581	PUSH Malware_.0040203C	
00401586	MOV EAX, DWORD PTR FS:[0]	SE handler installation
0040158C	PUSH EAX	
0040158D	MOV DWORD PTR FS:[0], ESP	
00401594	SUB ESP, 10	
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-18], ESP	
0040159A	CALL DWORD PTR DS:[<&kernel32.GetVersion	kernel32.GetVersion
0040159D	XOR EDX, EDX	
004015A5	MOV DL, AH	
004015A7	MOV DWORD PTR DS:[4052D4], EDX	
004015AD	MOV ECX, EAX	
004015AF	AND ECX, 0FF	
004015B5	MOV DWORD PTR DS:[4052D0], ECX	
004015B8	SHL ECX, 8	
004015BE	ADD ECX, EDX	
004015C0	MOV DWORD PTR DS:[4052CC], ECX	
004015C6	SHR EAX, 10	
004015C8	MOV EAX, 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



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

File View Debug Plugins Options Window Help

Assembly window (Address, Disassembly, Comment):

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV EBP, ESP	
0040157A	PUSH -1	
0040157C	PUSH Malware_.004040C0	
00401581	PUSH Malware_.0040203C	
00401586	MOV EAX, DWORD PTR FS:[0]	SE handler installation
0040158C	PUSH EAX	
0040158D	MOV DWORD PTR FS:[0], ESP	
00401594	SUB ESP, 10	
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-10], ESP	
0040159B	CALL DWORD PTR DS:[<<KERNEL32.GetVersion	kernel32.GetVersion
0040159E	XOR ECX, EDX	
004015A5	MOV DL, AH	
004015A7	MOV DWORD PTR DS:[4052D4], EDX	
004015AD	MOV ECX, EAX	
004015B0	AND ECX, 0FF	
004015B5	MOV DWORD PTR DS:[4052D0], ECX	
004015B8	SHL ECX, 8	
004015BE	ADD ECX, EDX	
004015C0	MOV DWORD PTR DS:[4052CC], ECX	
004015C6	SHR EAX, 10	
004015C9	MOV DWORD PTR DS:[4052C8], EAX	
004015CE	PUSH 0	
004015D0	CALL Malware_.00401F00	
004015D5	POP ECX	
004015D6	TEST EAX, EAX	
004015D9	JNZ SHORT Malware_.00401CF2	

Registers (FPU):

Register	Value
EAX	00280105
ECX	00000005
EDX	00000001
EBX	7FFDA000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910200 ntdll.7C910200
EIP	004015B5 Malware_.004015B5
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 0038 32bit 7FFCF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_INVALID_HANDLE (00000)
EFL	00000206 (NO, NB, NE, A, NS, PE, GE, G)
ST0	empty -UNORM BCBC 01050104 005C0030
ST1	empty +UNORM 0069 006E0069 002E0067
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0