

Esercizio S11-L3

All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1) ☐ Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5) ☐ Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

1. Il valore del parametro command line è «cmd»

0040105F	. 6A 00	PUSH 0	CreationFlags = 0
00401061	. 6A 01	PUSH 1	InheritHandles = TRUE
00401063	. 6A 00	PUSH 0	pThreadSecurity = NULL
00401065	. 6A 00	PUSH 0	pProcessSecurity = NULL
00401067	. 68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	. 6A 00	PUSH 0	ModuleFileName = NULL
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA]	CreateProcessA
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
00401077	. 6A FF	PUSH -1	Timeout = INFINITE
00401079	. 8B4D F0	MOV ECX, DWORD PTR SS:[EBP-10]	
0040107C	. 51	PUSH ECX	hObject

2. Il valore di EDX è 00000A28

00401577	. 57	PUSH EDI	
0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion]	kernel32.GetVersion
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C0	TEST EAX,EAX	
004015D8	. 75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015EB	. FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetCommand	CGetCo
004015F1	. A3 D8574000	MOV DWORD PTR DS:[4057D8],EAX	
004015F6	. E8 30060000	CALL Malware_.00401C2B	
004015FB	. A3 B0524000	MOV DWORD PTR DS:[4052B0],EAX	
00401600	. E8 D9030000	CALL Malware_.004019DE	
00401605	. E8 1B030000	CALL Malware_.00401925	
0040160A	. E8 90000000	CALL Malware_.0040169F	
0040160F	. A1 E4524000	MOV EAX, DWORD PTR DS:[4052E4]	
00401614	. A3 E8524000	MOV DWORD PTR DS:[4052E8],EAX	

EDX=00000A28

3. Dopo step into il valore di EDX è 0, a causa dell'istruzione XOR

00401577	. 55	PUSH EBP	
00401578	. 8BEC	MOV EBP,ESP	
0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	
00401586	. 64:A1 00000000	MOV EAX, DWORD PTR FS:[0]	SE handler installati
0040158C	. 50	PUSH EAX	
0040158D	. 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	
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion]	kernel32.GetVersion
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	

Registers (FPU)				
EAX	0A280105			
ECX	7FFDA000			
EDX	00000000			
EBX	7FFDA000			
ESP	0012FF8C			
EBP	0012FFC0			
ESI	FFFFFFFF			
EDI	7C920208	ntdll.7C920208		
EIP	004015A5	Malware_.004015		
C 0	ES 0023	32bit 0(FFFFFFF		
P 1	CS 001B	32bit 0(FFFFFFF		
A 0	SS 0023	32bit 0(FFFFFFF		
Z 1	DS 0023	32bit 0(FFFFFFF		
S 0	FS 003B	32bit 7FFDF000(
T 0	GS 0000	NULL		

- 4 Stesso procedimento di prima.
- 5 Il risultato di ECX dopo step into è 5, dopo l'istruzione AND che confronta i valori di ECX e 0FF che corrisponde a 256.

004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],ECX	
004015AD	. 8BC8	MOV ECX,EAX	
004015B0	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C0	TEST EAX,EAX	
004015D8	. 75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015EB	. FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetCommandLine	
004015F1	. A3 D8574000	MOV DWORD PTR DS:[4057D8],EAX	
004015F6	. E8 30060000	CALL Malware_.00401C2B	
004015FB	. A3 B0524000	MOV DWORD PTR DS:[4052B0],EAX	
00401600	. E8 D9030000	CALL Malware_.004019DE	
00401605	. E8 1B030000	CALL Malware_.00401925	
0040160A	. E8 90000000	CALL Malware_.0040169F	
0040160F	. A1 E4524000	MOV EAX,DWORD PTR DS:[4052E4]	
00401614	. A3 E8524000	MOV DWORD PTR DS:[4052E8],EAX	

ECX=0A280105

004015AD	. 8BC8	MOV ECX,EAX	
004015B0	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C0	TEST EAX,EAX	
004015D8	. 75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. 8365 FC 00	AND DWORD PTR SS:[EBP-4],0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015EB	. FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetCommandLine	
004015F1	. A3 D8574000	MOV DWORD PTR DS:[4057D8],EAX	
004015F6	. E8 30060000	CALL Malware_.00401C2B	
004015FB	. A3 B0524000	MOV DWORD PTR DS:[4052B0],EAX	
00401600	. E8 D9030000	CALL Malware_.004019DE	
00401605	. E8 1B030000	CALL Malware_.00401925	
0040160A	. E8 90000000	CALL Malware_.0040169F	
0040160F	. A1 E4524000	MOV EAX,DWORD PTR DS:[4052E4]	
00401614	. A3 E8524000	MOV DWORD PTR DS:[4052E8],EAX	

ECX=00000005
DS:[004052D0]=00000000