

S11 L3 OllyDBG

Traccia:

Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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)**.

Nella funzione "CreateProcessA", all'indirizzo 0040106E, il parametro "CommandLine" ha come valore "cmd".

00401056	. 52	PUSH EDX	pProcessInfo pStartupInfo CurrentDir = NULL pEnvironment = NULL CreationFlags = 0 InheritHandles = TRUE pThreadSecurity = NULL pProcessSecurity = NULL CommandLine = "cmd" ModuleFileName = NULL
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.CreatePro	
			CreateProcessA

Il valore del registro EDX all'indirizzo 004015A3 prima di effettuare questa operazione "XOR EDX, EDX" è di 00000A28

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
004015BB	. 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

L'istruzione XOR restituisce 1 per ogni coppia di bit diversi e 0 per ogni coppia di bit uguali, l'operazione viene effettuata tra EDX e sé stesso il risultato sarà 0. Azzerando così il valore di EDX.

				Registers (FPU)	
00401575	. C9	LEAVE		EAX	0A280105
00401576	. C3	RETN		ECX	7FFD7000
00401577	\$ 55	PUSH EBP		EDX	00000000
00401578	. 8BEC	MOV EBP,ESP		EBX	7FFD7000
0040157A	. 6A FF	PUSH -1		ESP	0012FF94
0040157C	. 68 C0404000	PUSH Malware_.004040C0		EBP	0012FFC0
00401581	. 68 3C204000	PUSH Malware_.0040203C	SE hanc	ESI	FFFFFFFF
00401586	. 64:A1 00000000	MOV EAX,DWORD PTR FS:[0]		EDI	7C920208 ntdll.7C920208
0040158C	. 50	PUSH EAX		EIP	004015A5 Malware_.004015A5
0040158D	. 64:8925 00000000	MOV DWORD PTR FS:[0],ESP		C 0	ES 0023 32bit 0(FFFFFFFF)
00401594	. 83EC 10	SUB ESP,10		P 1	CS 001B 32bit 0(FFFFFFFF)
00401597	. 53	PUSH EBX		A 0	SS 0023 32bit 0(FFFFFFFF)
00401598	. 56	PUSH ESI		Z 1	DS 0023 32bit 0(FFFFFFFF)
00401599	. 57	PUSH EDI		S 0	FS 003B 32bit 7FFDF000(FFF)
0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	kernel3	T 0	GS 0000 NULL
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion		D 0	
004015A3	. 33D2	XOR EDX,EDX			
004015A5	. 8AD4	MOV DL,AH			

Il valore del registro ECX all'indirizzo 004015AF prima di effettuare l'operazione "AND ECX, 0FF" è di 0A280105

004015AF	. 81E1 FF000000	AND ECX,0FF
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX
004015BB	. 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

ECX=0A280105

“AND ECX, 0FF”: L’operazione AND tra due operandi (A e B) restituirà 1 solo se entrambi A e B sono 1; in tutti gli altri casi, restituirà 0. ECX=00000005

004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015BB	. 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	

ECX=00000005