

Esercizio OllyDBG | Marco Malizia - DataShields

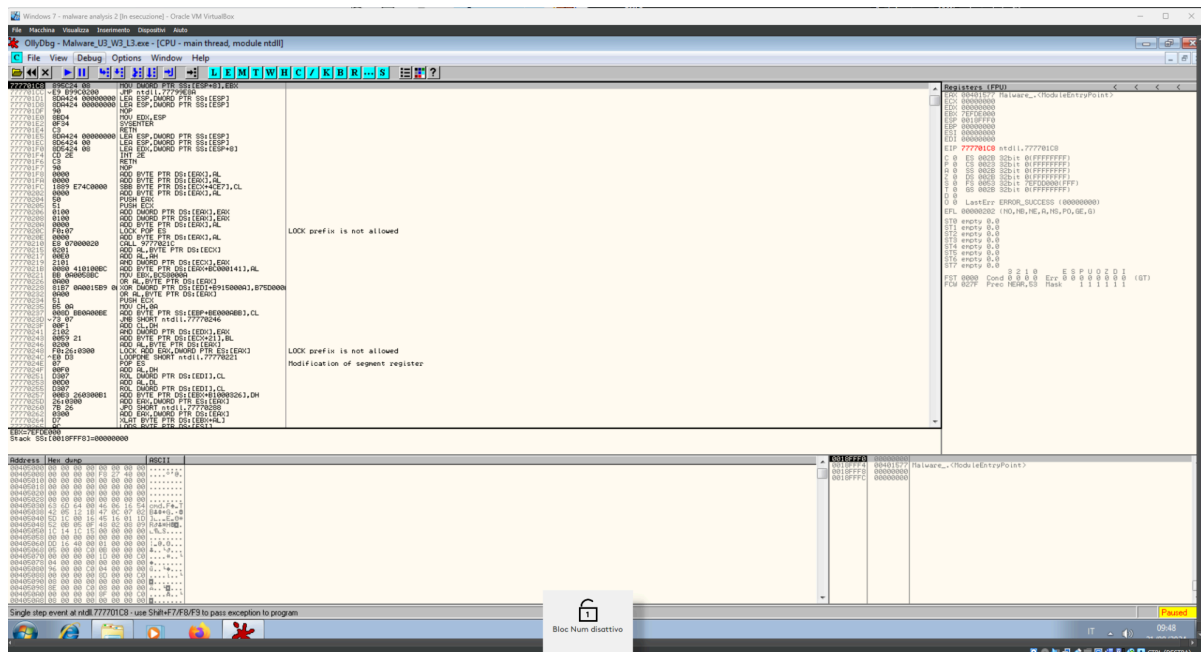
Traccia:

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul 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).
- BONUS: spiegare a grandi linee il funzionamento del malware

Svolgimento:

Avvio della macchina e del software OllyDBG.



1. 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?

Dopo aver aperto il file da analizzare andiamo a ricercare l'indirizzo indicato nella traccia. Il parametro di CommandLine è indicato nella quarta colonna e corrisponde a "cmd".

00401047	8B45 E8	MOV EAX, DWORD PTR SS:[EBP-20]	
0040104A	8945 E8	MOV DWORD PTR SS:[EBP-18], EAX	
0040104D	8B4D E8	MOV ECX, DWORD PTR SS:[EBP-18]	
00401050	894D E4	MOV DWORD PTR SS:[EBP-1C], ECX	
00401053	8D55 F0	LEA EDI, DWORD PTR SS:[EBP-10]	
00401056	52	PUSH EDI	
00401057	8D45 A8	LEA EAX, DWORD PTR SS:[EBP-58]	
0040105A	50	PUSH EAX	pProcessInfo
0040105B	6A 00	PUSH 0	pStartupInfo
0040105D	6A 00	PUSH 0	CurrentDir = NULL
0040105F	6A 00	PUSH 0	pEnvironment = NULL
00401061	6A 01	PUSH 1	CreationFlags = 0
00401063	6A 00	PUSH 0	InheritHandles = TRUE
00401065	6A 00	PUSH 0	pThreadSecurity = NULL
00401067	68 30504000	PUSH Malware_.00405030	pProcessSecurity = NULL
0040106C	6A 00	PUSH 0	CommandLine = "cmd"
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA>]	ModuleFileName = NULL
00401074	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA>]	CreateProcessA
00401077	6A FF	PUSH -1	Timeout = INFINITE
00401079	8B4D F0	MOV ECX, DWORD PTR SS:[EBP-10]	
0040107C	51	PUSH ECX	hObject
0040107D	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSingleObject>]	WaitForSingleObject
00401083	33C0	XOR EAX, EAX	
00401085	8BE5	MOV ESP, EBP	

2. 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)

Questa è la sequenza delle azioni, nella prima immagine andiamo ad identificare l'indirizzo oggetto di analisi.

0040158C	50	PUSH EAX	
00401590	64:925 000000	MOV DWORD PTR FS:[0], ESP	
00401594	83EC 10	SUB ESP, 10	
00401597	53	PUSH EBX	
00401598	53	PUSH EBX	
00401599	57	PUSH EDI	
0040159A	8B45 E8	MOV DWORD PTR SS:[EBP-18], ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A3	33D2	XOR EDI, EDI	
004015A5	8D45 A8	LEA EAX, DWORD PTR DS:[4052D4], EDI	
004015A7	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015A9	81E1 FF000000	AND ECX, 0	
004015AB	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015AD	81E1 00	SHL ECX, 8	
004015AE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	

In questa immagine mostriamo come andiamo ad inserire il "breakpoint".

0040158C	50	PUSH EAX	
00401590	64:925 000000	MOV DWORD PTR FS:[0], ESP	
00401594	83EC 10	SUB ESP, 10	
00401597	53	PUSH EBX	
00401598	53	PUSH EBX	
00401599	57	PUSH EDI	
0040159A	8B45 E8	MOV DWORD PTR SS:[EBP-18], ESP	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A3	33D2	XOR EDI, EDI	
004015A5	8D45 A8	LEA EAX, DWORD PTR DS:[4052D4], EDI	
004015A7	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015A9	81E1 FF000000	AND ECX, 0	
004015AB	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015AD	81E1 00	SHL ECX, 8	
004015AE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015B8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015BE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015C8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015CE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015D8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015DE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015E8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015EE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F0	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F2	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F4	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F6	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015F8	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FA	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FC	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	
004015FE	8B4D E8	MOV ECX, DWORD PTR DS:[4052D0], ECX	

Eseguendo il programma possiamo vedere come il valore del registro EDX è diventato **0001DB1**.

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]	
0040158C	PUSH EAX	
00401590	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	
0040159D	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A3	XOR EDX, EDX	
004015A5	MOV DL, AH	

Register	Value
EAX	1DB10106
ECX	7EFD0000
EDX	00001DB1
EBX	7EFD0000
ESP	0018FF5C
EBP	0018FF58
ESI	00000000
EDI	00000000
EIP	004015A3

Utilizzando la funzione “Step-into” nella barra degli strumenti, che permette di entrare nel codice della funzione in esame, abbiamo notato che il valore EDX nel registro è mutato in **00000000**

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]	
0040158C	PUSH EAX	
00401590	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	
0040159D	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A3	XOR EDX, EDX	
004015A5	MOV DL, AH	
004015A7	MOV DWORD PTR DS:[4052D4], EDX	

Register	Value
EAX	1DB10106
ECX	7EFD0000
EDX	00000000
EBX	7EFD0000
ESP	0018FF5C
EBP	0018FF58
ESI	00000000
EDI	00000000
EIP	004015A5

Questo cambiamento è dovuto all'operazione logica XOR nel codice, che restituisce sempre 0 quando applicata a due valori uguali. In questo caso, l'operazione XOR ha annullato il valore precedente di EDX, impostandolo a zero.

3. 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).

00401577 <ModuleEntryP	55	PUSH EBP		
00401578	8BEC	MOV EBP,ESP		
00401579	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 installation	
0040158C	50	PUSH EAX		
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	33EC 10	SUB ESP,10		
00401597	53	PUSH EBX		
00401598	56	PUSH ESI		
00401599	57	PUSH EDI		
0040159A	9965 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	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	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX		

Configuro il secondo breakpoint, il valore del registro ECX è 1DB10106

00401577 <ModuleEntryP	55	PUSH EBP		
00401578	8BEC	MOV EBP,ESP		
00401579	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 installation	
0040158C	50	PUSH EAX		
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	33EC 10	SUB ESP,10		
00401597	53	PUSH EBX		
00401598	56	PUSH ESI		
00401599	57	PUSH EDI		
0040159A	9965 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	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	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX		

Dopo lo step-into il valore del registro ECX è stato modificato in 00000006 in quanto è stata eseguita l'istruzione AND ECX, FF.

In questo caso c'è un operato logico AND il quale ricevendo in ingresso almeno due valori restituisce 1 solo se tutti i valori di ingresso hanno valore

00401577 <ModuleEntryP	55	PUSH EBP		
00401578	8BEC	MOV EBP,ESP		
00401579	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 installation	
0040158C	50	PUSH EAX		
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP		
00401594	33EC 10	SUB ESP,10		
00401597	53	PUSH EBX		
00401598	56	PUSH ESI		
00401599	57	PUSH EDI		
0040159A	9965 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	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	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX		