

# Esercitazione WEEK W24D1

## OllyDBG

Ettore Farris

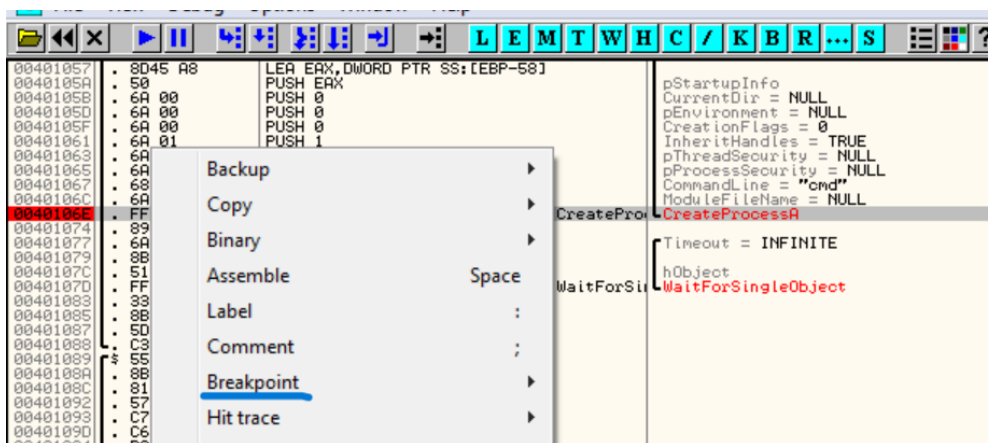
### Descrizione sintetica e risoluzione

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)**

Una volta aperto il debugger e caricato l'eseguibile, settiamo il breakpoint all'indirizzo 0040106E ed avviamo l'esecuzione. Sullo stack possiamo vedere che il parametro *CommandLine* ha valore "cmd".



0018FF58	00000000	ModuleFileName = NULL
0018FF5C	00000000	CommandLine = "cmd"
0018FF60	00000000	pProcessSecurity = NULL
0018FF64	00000000	pThreadSecurity = NULL
0018FF68	00000001	InheritHandles = TRUE
0018FF7C	00000000	CreationFlags = 0
0018FF80	00000000	pEnvironment = NULL
0018FF84	00000000	CurrentDir = NULL
0018FF88	0018FF90	pStartupInfo = 0018FF90
0018FF8C	0018FFD8	pProcessInfo = 0018FFD8
0018FF90	00000044	
0018FF94	00000000	
0018FF98	00000000	
0018FF9C	00000000	
0018FFA0	00000000	
0018FFA4	00000000	

- **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)**

Una volta settato il breakpoint, il valore di EDX è 00001DB1. L'istruzione effettua una XOR EDX, EDX settando quindi il registro a 0. Eseguita l'istruzione quindi, il valore del registro EDX viene azzerato.

Prima dell'esecuzione

00401577	65	PUSH EBP		EIP 004015A3	Malware_.004015A3
00401578	8BEC	MOV EBP, ESP		C 0	ES 002B 32bit 0(FFFFFFFF)
0040157A	6A FF	PUSH -1		P 1	CS 002B 32bit 0(FFFFFFFF)
0040157C	68 00404000	PUSH Malware_.00404000		A 0	SS 002B 32bit 0(FFFFFFFF)
00401581	68 3C204000	PUSH Malware_.0040203C		Z 0	DS 002B 32bit 0(FFFFFFFF)
00401586	64:41 00000000	MOV EAX, DWORD PTR FS:[0]	SE handler installation	S 0	FS 0053 32bit 7EFD0000(FFF)
0040158C	50	PUSH EAX		T 0	GS 002B 32bit 0(FFFFFFFF)
0040158D	64:8925 000000	MOV DWORD PTR FS:[0], ESP		O 0	LastErr ERROR_SUCCESS (00000000)
00401594	83EC 10	SUB ESP, 10	kernel32.GetVersion	EFL	00000206 (NO, NB, NE, A, NS, PE, G)
00401597	53	PUSH EBX		MM0	0.0, 0.0
00401598	56	PUSH ESI		MM1	0.0, 0.0
00401599	57	PUSH EDI		MM2	0.0, 0.0
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-10], ESP		MM3	0.0, 0.0
0040159D	FF15 30404000	CALL DWORD PTR DS:[<I>kernel32.GetVersion		MM4	0.0, 0.0
004015A3	33D2	XOR EDX, EDX		MM5	0.0, 0.0
004015A5	8AD4	MOV DL, AH		MM6	0.0, 0.0
004015A6	8B45 00404000	MOV ECX, DWORD PTR DS:[00404000], EDX			
004015AD	8BC8	MOV ECX, EAX			
004015AF	81E1 FF000000	AND ECX, 0			
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0], ECX			
004015B8	C1E1 08	SHL ECX, 5			
004015BE	03CA	ADD ECX, EDX			
004015C0	8900 CC524000	MOV DWORD PTR DS:[4052CC], ECX			
004015C6	C1E8 10	SHR ECX, 10			
004015C9	8B 00 00000000	MOV DWORD PTR DS:[4052C9], ECX			

Dopo l'esecuzione

Address	Disassembly	Comment
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]
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
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

Register	Value
EAX	1DB10106
ECX	1DB10106
EDX	00000000
EBX	7EFD0000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015A5
CS	002B
SS	002B
DS	002B
FS	0053
GS	002B
LastErr	ERROR_SUC
EFL	0000246

- **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).**

A partire dal punto precedente, impostiamo il breakpoint su 004015AF. Il valore del registro ECX è 1DB10106 (in binario 0001 1101 1011 0001 0000 0001 0000 0110).

Address	Disassembly	Comment
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]
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
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	83CA	ADD ECX,EDX
004015C0	890D CC524000	MOV DWORD PTR DS:[4052CC],ECX

Register	Value
EAX	1DB10106
ECX	1DB10106
EDX	00000001
EBX	7EFD0000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015AF
CS	002B
SS	002B
DS	002B
FS	0053
GS	002B
LastErr	ERROR_SUC
EFL	0000246

Effettuando la *step-into*, viene eseguita un'istruzione AND tra il valore del registro ECX e il valore esadecimale 0FF (0000 0000 0000 0000 0000 0000 1111 1111 in binario usando 32 bit). Quindi, l'AND *bitwise* (cioè bit a bit) tra:

- 0000 0000 0000 0000 0000 0000 1111 1111

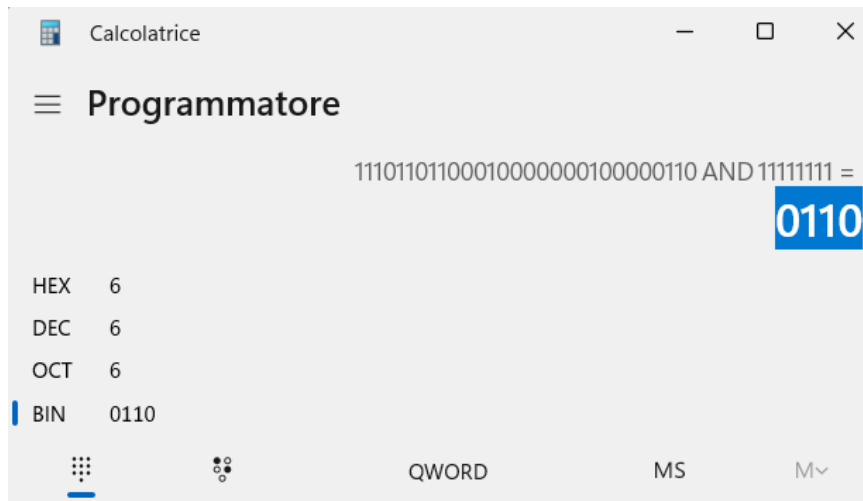
e

- 0001 1101 1011 0001 0000 0001 0000 0110

corrisponde a:

0000 0000 0000 0000 0000 0000 0000 0110

che in esadecimale vale 6.



Eseguendo l'istruzione, il valore del registro ECX vale infatti 6.

