

# Esercitazione W24D1 - Pratica 1

## Ollydbg

Fabio Benevento - 16/04/2024

---

### Traccia

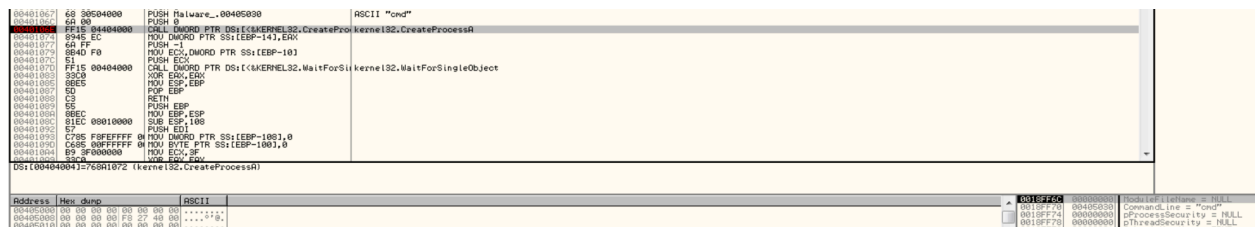
Fate riferimento al malware: Malware\_U3\_W3\_L3, presente all'interno della cartella Esercizio\_Pratico\_U3\_W3\_L3 sul desktop della macchina virtuale dedicata all'analisi dei malware.

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).

## Svolgimento

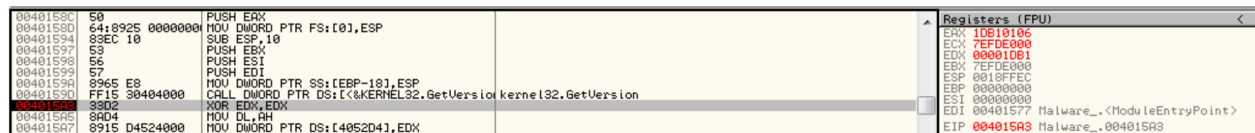
- Posizionando un breakpoint all'istruzione indicata ed eseguendo il codice fino ad esso è possibile visualizzare nella sezione in basso a destra il valore assunto dal parametro CommandLine che risulta essere pari a "cmd"



Address	Hex	dump	ASCII
00401067	68 00504000	PUSH Malware_.00405000	ASCII "cmd"
00401068	68 00	PUSH 0	
00401069	FF15 00404000	CALL DWORD PTR DS:[<&kernel32.CreateProcessA]	kernel32.CreateProcessA
0040106A	5B45 E2	MOV DWORD PTR SS:[EBP+14],EAX	
0040106B	6A F0	PUSH -F0	
0040106C	5B	MOV ECX, DWORD PTR SS:[EBP-10]	
0040106D	51	PUSH EAX	
0040106E	FF15 00404000	CALL DWORD PTR DS:[<&kernel32.WaitForSingleObject]	kernel32.WaitForSingleObject
0040106F	5BCB	MOV EAX, EBP	
00401070	5BCB	MOV EAX, EBP	
00401071	5B	POP EBP	
00401072	C3	RETN	
00401073	66	PUSH EBP	
00401074	5BEC	MOV ESP, EBP	
00401075	5BEC	MOV ESP, 100	
00401076	57	PUSH EDI	
00401077	C78E FFFFFFFF	MOV DWORD PTR SS:[EBP-100],0	
00401078	CAB5 00FFFFFF	MOV BYTE PTR SS:[EBP-100],0	
00401079	59	POP EAX	
0040107A	59	POP EAX	

Register	Value
EAX	1DB10106
ECX	7EFDE000
EDX	00001DB1
EBX	7EFDE000
ESP	0018FFEC
EBP	00000000
ESI	00000000
EDI	00401577 Malware_.<ModuleEntryPoint>
EIP	004015A3 Malware_.004015A3

- Posizionando un breakpoint all'istruzione 004015A3 ed eseguendo il codice fino al punto del breakpoint prima della nostra esecuzione, il valore del registro EDX assunto è pari a 0x00001DB1



Address	Hex	dump	ASCII
0040158C	50	PUSH EAX	
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
0040158E	83EC 10	SUB ESP,10	
0040158F	53	PUSH EBX	
00401590	56	PUSH ESI	
00401591	57	PUSH EDI	
00401592	9965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
00401593	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion]	kernel32.GetVersion
00401594	3302	XOR EDX,EDX	
00401595	9044	MOV DL,AH	
00401596	8915 D4520400	MOV DWORD PTR DS:[405204],EDX	

Register	Value
EAX	1DB10106
ECX	7EFDE000
EDX	00000000
EBX	7EFDE000
ESP	0018FFEC
EBP	00000000
ESI	00000000
EDI	00000000
EIP	004015A5 Malware_.004015A5

Eseguendo uno step-into ed andando quindi al punto successivo il registro EDX assume il valore 0x00000000 come evidenziato in figura



Address	Hex	dump	ASCII
0040156B	74 04	JE SHORT Malware_.00401571	
0040156C	3309	XOR EAX,EAX	
0040156D	EB 02	JMP SHORT Malware_.00401573	
0040156E	8BC7	MOV EAX,EDI	
0040156F	FC	CLD	
00401570	5F	POP EDI	
00401571	C9	LEAVE	
00401572	C3	RETN	
00401573	55	PUSH EBP	
00401574	5BEC	MOV EBP,ESP	
00401575	6A FF	PUSH -1	
00401576	68 C0404000	PUSH Malware_.004040C0	
00401577	68 3C204000	PUSH Malware_.0040203C	
00401578	64:A1 00000000	MOV EAX, DWORD PTR FS:[0]	
00401579	50	PUSH EAX	
0040157A	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
0040157B	83EC 10	SUB ESP,10	
0040157C	53	PUSH EBX	
0040157D	56	PUSH ESI	
0040157E	57	PUSH EDI	
0040157F	9965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
00401580	FF15 30404000	CALL DWORD PTR DS:[<&kernel32.GetVersion]	kernel32.GetVersion
00401581	3302	XOR EDX,EDX	
00401582	9044	MOV DL,AH	
00401583	8915 D4520400	MOV DWORD PTR DS:[405204],EDX	
00401584	8BC8	MOV ECX,EAX	

Register	Value
EAX	1DB10106
ECX	7EFDE000
EDX	00000000
EBX	7EFDE000
ESP	0018FFEC
EBP	00000000
ESI	00000000
EDI	00000000
EIP	004015A5 Malware_.004015A5

Ciò è dovuto al fatto in quanto l'istruzione su cui era posizionato il breakpoint ed eseguita in seguito all'operazione step-into, ovvero XOR EDX, EDX, esegue l'operazione XOR tra due valori uguali e quindi di fatto equivale a porre il registro a 0.

- Posizionando un breakpoint all'istruzione 004015A3 ed eseguendo il codice fino al punto del breakpoint prima della nostra esecuzione, il valore del registro ECX assunto è pari a 0x1DB10106 come mostrato in figura

0040159C	50	PUSH EAX	
0040159D	64:8925 00000	MOV DWORD PTR FS:[0],ESP	
0040159E	83EC 10	SUB ESP,10	
0040159F	53	PUSH EBX	
004015A0	56	PUSH ESI	
004015A1	57	PUSH EDI	
004015A2	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
004015A3	FF15 30404000	CALL DWORD PTR DS:[4052D4],kernel32.GetVersion	kernel32.GetVersion
004015A4	3302	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A6	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A7	8BC9	MOV ECX,EAX	
004015A8	81E1 FF000000	AND ECX,0FF	
004015A9	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015AA	C1E1 08	SHL ECX,8	
004015AB	8BC9	MOV ECX,EDX	
004015AC	8900 CC524000	MOV DWORD PTR DS:[4052C0],ECX	

Registers (FPU)				
EAX	10B10106			
ECX	00000006			
EDX	00000001			
EBX	7EFDE000			
ESP	0018FF5C			
EBP	0018FF58			
ESI	00000000			
EDI	00000000			
EIP	004015AF	Malware_.004015AF		
C 0	ES 002B	32bit 0(FFFFFFFF)		
P 1	CS 0023	32bit 0(FFFFFFFF)		
A 0	SS 002B	32bit 0(FFFFFFFF)		
Z 1	DS 002B	32bit 0(FFFFFFFF)		
S 0	FS 0053	32bit 7EFD0000(FFF)		
A	002B	32bit 0(FFFFFFFF)		

Eseguendo uno step-into ed andando quindi al punto successivo il registro ECX assume in questo caso il valore 0x00000006

0040159C	50	PUSH EAX	
0040159D	64:8925 00000	MOV DWORD PTR FS:[0],ESP	
0040159E	83EC 10	SUB ESP,10	
0040159F	53	PUSH EBX	
004015A0	56	PUSH ESI	
004015A1	57	PUSH EDI	
004015A2	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
004015A3	FF15 30404000	CALL DWORD PTR DS:[4052D4],kernel32.GetVersion	kernel32.GetVersion
004015A4	3302	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A6	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A7	8BC9	MOV ECX,EAX	
004015A8	81E1 FF000000	AND ECX,0FF	
004015A9	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015AA	C1E1 08	SHL ECX,8	
004015AB	8BC9	MOV ECX,EDX	
004015AC	8900 CC524000	MOV DWORD PTR DS:[4052C0],ECX	

Registers (FPU)				
EAX	10B10106			
ECX	00000006			
EDX	00000001			
EBX	7EFDE000			
ESP	0018FF5C			
EBP	0018FF58			
ESI	00000000			
EDI	00000000			
EIP	004015B5	Malware_.004015B5		
C 0	ES 002B	32bit 0(FFFFFFFF)		
P 1	CS 0023	32bit 0(FFFFFFFF)		
A 0	SS 002B	32bit 0(FFFFFFFF)		
Z 1	DS 002B	32bit 0(FFFFFFFF)		
S 0	FS 0053	32bit 7EFD0000(FFF)		
A	002B	32bit 0(FFFFFFFF)		

L'istruzione eseguita in questo caso è l'istruzione AND ECX, 0xFF che equivale e prelevare il solo byte meno significativo del registro e quindi il valore 0x06