

CONSEGNA SETTIMANA 11 LEZIONE 3

Malware analysis – OllyDBG

Ci viene richiesto di rispondere ai seguenti quesiti utilizzando OllyDBG

- **PUNTO 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?
- **PUNTO 2.** Inserite un breakpoint software all'indirizzo **004015A3**. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
- **PUNTO 3.** Inserite un secondo breakpoint all'indirizzo di memoria **004015AF**. Qual è il valore del registro **ECX**? Eseguite un step-into. Qual è ora il valore di **ECX**? Spiegate quale istruzione è stata eseguita.
- **BONUS:** spiegare a grandi linee il funzionamento del malware.

PUNTO 1.

Tramite il software **OllyDBG** ci è possibile analizzare dinamicamente il malware, soffermandoci sulle fasi dell'esecuzione che più ci interessano. Prendiamo in esame la chiamata alla funzione **CreateProcess** all'indirizzo 0040106E. Il valore del parametro **CommandLine** passato alla funzione in questo caso risulta essere **"cmd"**.

00401056	. 52	PUSH EDX	pProcessInfo
00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	pStartupInfo
0040105A	. 50	PUSH EAX	CurrentDir = NULL
0040105B	. 6A 00	PUSH 0	pEnvironment = NULL
0040105D	. 6A 00	PUSH 0	CreationFlags = 0
0040105F	. 6A 00	PUSH 0	InheritHandles = TRUE
00401061	. 6A 01	PUSH 1	pThreadSecurity = NULL
00401063	. 6A 00	PUSH 0	pProcessSecurity = NULL
00401065	. 6A 00	PUSH 0	ModuleFileName = 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

PUNTO 2.

Dopo aver inserito un breakpoint all'indirizzo **004015A3** come da istruzioni, possiamo notare il valore di **EDX**, ovvero **00001DB1**. Eseguendo poi il comando **step-into**, possiamo notare che il valore diventa 0. Questo avviene a causa dell'istruzione presente proprio all'indirizzo **0004015A3**, cioè **XOR EDX,EDX**. Lo XOR è una funzione logica che risulta in valore uguale a 1 se i parametri a confronto sono diversi tra loro, ma essendo EDX sempre uguale a EDX il risultato sarà 0.

00401577	. 55	PUSH EBP	SE handler installation
00401578	. 8BEC	MOV EBP,ESP	
0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	
00401586	. 41 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	. 50	PUSH EAX	
0040158D	. 64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	. 83EC 10	SUB ESP,10	
00401597	. 56	PUSH EAX	
00401598	. 56	PUSH EAX	
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	. 33DB	XOR EDX,EDX	
004015A5	. 8D44	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 89D0 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 89D0 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 38090000	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 EAX	

Registers (FPU)
EAX 1DB10106
ECX 7EFD0000
EDX 00001DB1
EBX 7EFD0000
ESP 0018FFFC
EBP 0018FFFC
ESI 00000000
EDI 00000000
EIP 004015A3 Malware_.004015A3
C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 0 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 7EFD0000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0
LastErr ERROR_SUCCESS (00000000)
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)
ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

00401576	. C9	LEAVE			
00401576	. C3	RETN			
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 installation		
0040158C	. 50	PUSH EAX			
0040158D	. 64:8925 000000	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			
0040159B	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion		
0040159B	. 33D2	XOR EDX,EDX			
004015A7	. 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	. 89B0 D0524000	MOV DWORD PTR DS:[4052D0],ECX			
004015B8	. C1E1 08	SHL ECX,8			
004015BE	. 03CA	ADD ECX,EDX			
004015C0	. 89B0 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			
004015DD	. 6A 1C	PUSH 1C			

Registers (FPU)			
EAX	1DB10106		
ECX	7EFD0000		
EDX	00000000		
EBX	7EFD0000		
ESP	0018FF5C		
EBP	0018FF88		
ESI	00000000		
EDI	00000000		
EIP	004015A5	Malware_.004015A5	
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)	
T 0	GS 002B	32bit 0(FFFFFFFF)	
D 0			
O 0	LastErr	ERROR_SUCCESS (00000000)	
EFL	00000246	(NO,NB,E,BE,NS,PE,GE,LE)	
ST0	empty	0.0	
ST1	empty	0.0	
ST2	empty	0.0	
ST3	empty	0.0	
ST4	empty	0.0	
ST5	empty	0.0	
ST6	empty	0.0	
ST7	empty	0.0	
FST	0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)	
FCW	027F	Prec NEAR,53 Mask 1 1 1 1 1 1	

PUNTO 3.

Analogamente, inserendo un breakpoint all'indirizzo **004015AF**, notiamo che il valore di **ECX** sia **1DB10106**. Eseguendo uno step-into possiamo constatare che il valore cambia e diventa **00000006**. Questo avviene a causa proprio dell'operazione all'indirizzo 004015AF, ovvero **AND EXC, 0FF**. L'operatore logico AND in questo caso confronta tra di loro i singoli bit dei due valori, ovvero ECX e 0FF. Per confermare ciò convertiamo prima i valori di ECX e il valore 0FF in binario.

ECX 1DB10106 (exa) -> 0001 1101 1011 0001 0000 0001 0000 0110

0FF (exa) -> 0000 0000 0000 0000 0000 0000 1111 1111

A questo punto poniamo l'AND logico bit per bit e otteniamo il valore 0000 0000 0000 0000 0000 0000 0110, ovvero 00000006.

00401576	. C9	LEAVE			
00401576	. C3	RETN			
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 installation		
0040158C	. 50	PUSH EAX			
0040158D	. 64:8925 000000	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			
0040159B	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion		
004015A5	. 8AD4	MOV DL,AH			
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX			
004015AD	. 8BC8	MOV ECX,EAX			
004015B5	. 81E1 FF000000	AND ECX,0FF			
004015B8	. 89B0 D0524000	MOV DWORD PTR DS:[4052D0],ECX			
004015BB	. C1E1 08	SHL ECX,8			
004015BE	. 03CA	ADD ECX,EDX			
004015C0	. 89B0 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			
004015DD	. 6A 1C	PUSH 1C			

Registers (FPU)			
EAX	1DB10106		
ECX	1DB10106		
EDX	00000000		
EBX	7EFD0000		
ESP	0018FF5C		
EBP	0018FF88		
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)	
T 0	GS 002B	32bit 0(FFFFFFFF)	
D 0			
O 0	LastErr	ERROR_SUCCESS (00000000)	
EFL	00000246	(NO,NB,E,BE,NS,PE,GE,LE)	
ST0	empty	0.0	
ST1	empty	0.0	
ST2	empty	0.0	
ST3	empty	0.0	
ST4	empty	0.0	
ST5	empty	0.0	
ST6	empty	0.0	
ST7	empty	0.0	
FST	0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)	
FCW	027F	Prec NEAR,53 Mask 1 1 1 1 1 1	

00401576	. C9	LEAVE			
00401576	. C3	RETN			
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 installation		
0040158C	. 50	PUSH EAX			
0040158D	. 64:8925 000000	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			
0040159B	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion		
004015A5	. 8AD4	MOV DL,AH			
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX			
004015AD	. 8BC8	MOV ECX,EAX			
004015B5	. 81E1 FF000000	AND ECX,0FF			
004015B8	. 89B0 D0524000	MOV DWORD PTR DS:[4052D0],ECX			
004015BB	. C1E1 08	SHL ECX,8			
004015BE	. 03CA	ADD ECX,EDX			
004015C0	. 89B0 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			
004015DD	. 6A 1C	PUSH 1C			

Registers (FPU)			
EAX	00000006		
ECX	00000006		
EDX	00000000		
EBX	7EFD0000		
ESP	0018FF5C		
EBP	0018FF88		
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 0	DS 002B	32bit 0(FFFFFFFF)	
S 0	FS 0053	32bit 7EFD0000(FFF)	
T 0	GS 002B	32bit 0(FFFFFFFF)	
D 0			
O 0	LastErr	ERROR_SUCCESS (00000000)	
EFL	00000206	(NO,NB,NE,A,NS,PE,GE,G)	
ST0	empty	0.0	
ST1	empty	0.0	
ST2	empty	0.0	
ST3	empty	0.0	
ST4	empty	0.0	
ST5	empty	0.0	
ST6	empty	0.0	
ST7	empty	0.0	
FST	0000	Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)	
FCW	027F	Prec NEAR,53 Mask 1 1 1 1 1 1	