

2024



CS0124

REPORT

Week 11 Lesson 3

PREPARED BY : Bruno Falconi

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 del 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

- 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)

All'indirizzo specificato il malware effettua una chiamata di funzione, alla funzione «**CreateProcess**» il valore del parametro che viene passato sullo stack è «**cmd**» il che ci fa supporre che stia aprendo una shell.

- 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)

Il valore è **00001DB1** e dopo diventa **0** in quanto effettua uno **XOR** su se stesso e quindi il valore risulta zero successivamente.

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

LEMTWHC / KBR... S

Address	Disassembly	Comment
0040158B	XOR EDX,EDX	
004015A5	MOV DL,AH	
004015A7	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	MOV ECX,EAX	
004015AF	AND ECX,0FF	
004015B5	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	SHL ECX,8	
004015BE	ADD ECX,EDX	
004015C0	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	SHR EAX,10	
004015C9	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	PUSH 0	
004015D0	CALL Malware_.00401F08	
004015D5	POP ECX	
004015D6	TEST EAX,EAX	
004015D8	JNZ SHORT Malware_.004015E2	
004015DA	PUSH 1C	
004015DC	CALL Malware_.0040167B	
004015E1	POP ECX	
004015E2	AND DWORD PTR SS:[EBP-4],0	
004015E6	CALL Malware_.00401D5D	
004015EB	CALL DWORD PTR DS:[&KERNEL32.GetCommandLineA	CGetCommandLineA
004015F1	MOV DWORD PTR DS:[4057D8],EAX	
004015F8	CALL Malware_.00401C2B	
00401600	MOV DWORD PTR DS:[4052B0],EAX	
00401605	CALL Malware_.004019DE	
0040160A	CALL Malware_.00401925	
0040160F	CALL Malware_.0040169F	
00401614	MOV EAX,DWORD PTR DS:[4052E4]	
00401619	MOV DWORD PTR DS:[4052E8],EAX	
0040161A	PUSH EAX	
0040161B	PUSH DWORD PTR DS:[4052DC]	
00401620	PUSH DWORD PTR DS:[4052D8]	
00401626	CALL Malware_.00401128	
0040162B	ADD ESP,0C	
0040162E	MOV DWORD PTR SS:[EBP-1C],EAX	
00401631	PUSH EAX	
00401632	CALL Malware_.004016CC	
00401637	MOV EAX,DWORD PTR SS:[EBP-14]	
0040163A	MOV ECX,DWORD PTR DS:[EAX]	
0040163C	MOV ECX,DWORD PTR DS:[ECX]	
0040163E	MOV DWORD PTR SS:[EBP-20],ECX	
00401641	PUSH EAX	
00401642	PUSH ECX	
00401643	CALL Malware_.004017A1	
00401648	POP ECX	
00401649	POP ECX	
0040164A	RETN	
0040164B	DB 8B	
0040164C	DB 65	CHAR 'e'
0040164D	DB E8	
0040164E	DB FF	
0040164F	DB 75	CHAR 'u'
00401650	DB E0	
00401651	DB 59	

Registers (F)

Register	Value
EAX	1DB10106
ECX	7EFDE000
EDX	000010B1
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF58
ESI	00000000
EDI	00000000
EIP	004015A3
C 0	ES 002B
P 1	CS 0023
A 0	SS 002B
Z 0	DS 002B
S 0	FS 0053
T 0	GS 002B
D 0	
O 0	LastErr
EFL	00000206
ST0	empty 0.
ST1	empty 0.
ST2	empty 0.
ST3	empty 0.
ST4	empty 0.
ST5	empty 0.
ST6	empty 0.
ST7	empty 0.
FST	0000 Co
FCW	027F Pa

EDX=000010B1

Malware_.<ModuleEntryPoint>+2C

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

LEMTWHC / KBR... S

004015A5	83D2	XOR EDX, EDX		
004015A6	8AD4	MOV DL, AH		
004015A7	8915	MOV DWORD PTR DS:[4052D4], EDX		
004015A8	8BC8	MOV ECX, EAX		
004015A9	81E1	AND ECX, 0FF		
004015AB	89D0	MOV DWORD PTR DS:[4052D0], ECX		
004015AC	C1E1	SHL ECX, 8		
004015AD	03CA	ADD ECX, EDX		
004015AE	89D0	MOV DWORD PTR DS:[4052CC], ECX		
004015AF	C1E8	SHR EAX, 10		
004015B0	A3	MOV DWORD PTR DS:[4052C8], EAX		
004015B1	6A	PUSH 0		
004015B2	E8	CALL Malware_.00401F08		
004015B3	59	POP ECX		
004015B4	85C0	TEST EAX, EAX		
004015B5	75	JNZ SHORT Malware_.004015E2		
004015B6	6A	PUSH 1C		
004015B7	E8	CALL Malware_.0040167B		
004015B8	59	POP ECX		
004015B9	8365	AND DWORD PTR SS:[EBP-4], 0		
004015BA	E8	CALL Malware_.00401D5D		
004015BB	FF15	CALL DWORD PTR DS:[<&KERNEL32.GetCommand	CGetCommandLineA	
004015BC	A3	MOV DWORD PTR DS:[4057D8], EAX		
004015BD	E8	CALL Malware_.00401C2B		
004015BE	A3	MOV DWORD PTR DS:[4052B0], EAX		
004015BF	E8	CALL Malware_.004019DE		
004015C0	E8	CALL Malware_.00401925		
004015C1	E8	CALL Malware_.0040169F		
004015C2	A1	MOV EAX, DWORD PTR DS:[4052E4]		
004015C3	A3	MOV DWORD PTR DS:[4052E8], EAX		
004015C4	50	PUSH EAX		
004015C5	FF35	PUSH DWORD PTR DS:[4052DC]		
004015C6	FF35	PUSH DWORD PTR DS:[4052D8]		
004015C7	E8	CALL Malware_.00401128		
004015C8	83C4	ADD ESP, 0C		
004015C9	8945	MOV DWORD PTR SS:[EBP-1C], EAX		
004015CA	50	PUSH EAX		
004015CB	E8	CALL Malware_.004016CC		
004015CC	8B45	MOV EAX, DWORD PTR SS:[EBP-14]		
004015CD	8B08	MOV ECX, DWORD PTR DS:[EAX]		
004015CE	8B09	MOV ECX, DWORD PTR DS:[ECX]		
004015CF	894D	MOV DWORD PTR SS:[EBP-20], ECX		
004015D0	50	PUSH EAX		
004015D1	51	PUSH ECX		
004015D2	E8	CALL Malware_.004017A1		
004015D3	59	POP ECX		
004015D4	59	POP ECX		
004015D5	C3	RETN		
004015D6	C3	RETN		
004015D7	65	DB 65	CHAR 'e'	
004015D8	E8	DB E8		
004015D9	FF	DB FF		
004015DA	75	DB 75	CHAR 'u'	
004015DB	E0	DB E0		
004015DC	E8	DB E8		

Registers (FPU)

EAX 10B10106
ECX 7EFD0000
EDX 00000000
EBX 7EFD0000
ESP 0018FFFC
ESI 00000000
EDI 00000000
EIP 004015A5
C 0 ES 002B
P 1 CS 0023
A 0 SS 002B
Z 1 DS 002B
S 0 FS 0053
T 0 GS 002B
D 0
I 0 LastErr
EFL 00010246
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 Con
FCW 027F Pre

Arg3 => 00000000
Arg2 = 00000000
Arg1 = 00000000
Malware_.00401128

CHAR 'e'
CHAR 'u'

Malware_.<ModuleEntryPoint>+2E

Address Hex dump ASCII

• 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).

Il valore iniziale è 10B10106 che diventa 00000000

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

LEMTWHC / KBR ... S

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	kernel32.GetVersion
004015A3	. 3302	XOR EDX, EDX	
004015A5	. 8A04	MOV DL, AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4], EDX	
004015A8	. 8BC8	MOV ECX, EAX	
004015B0	. 81E1 FF000000	AND ECX, 0FF	
004015B5	. 8960 D0524000	MOV DWORD PTR DS:[4052D0], ECX	
004015B8	. C1E1 08	SHL ECX, 8	
004015BE	. 03CA	ADD ECX, EDX	
004015C0	. 8960 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	. 75C0	TEST EAX, EAX	
004015D8	. 75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. 8365 FC 00	AND DWORD PTR SS:[EBP-4], 0	
004015E6	. E8 72070000	CALL Malware_.00401D5D	
004015EB	. FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetCommand	CGetCommandLineA
004015F1	. A3 D8574000	MOV DWORD PTR DS:[4057D8], EAX	
004015F6	. E8 30060000	CALL Malware_.00401C2B	
004015FB	. A3 B0524000	MOV DWORD PTR DS:[4052B0], EAX	
00401600	. E8 D9030000	CALL Malware_.004019DE	
00401605	. E8 1B030000	CALL Malware_.00401925	
0040160A	. E8 90000000	CALL Malware_.0040169F	
0040160F	. A1 E4524000	MOV EAX, DWORD PTR DS:[4052E4]	
00401614	. A3 E8524000	MOV DWORD PTR DS:[4052E8], EAX	
00401619	. 50	PUSH EAX	
0040161A	. FF35 DC524000	PUSH DWORD PTR DS:[4052DC]	
00401620	. FF35 D8524000	PUSH DWORD PTR DS:[4052D8]	
00401626	. E8 F0FAFFFF	CALL Malware_.00401128	
0040162B	. 83C4 0C	ADD ESP, 0C	
0040162E	. 8945 E4	MOV DWORD PTR SS:[EBP-1C], EAX	
00401631	. 50	PUSH EAX	
00401632	. E8 95000000	CALL Malware_.004016CC	
00401637	. 8B45 EC	MOV EAX, DWORD PTR SS:[EBP-14]	
0040163A	. 8B08	MOV ECX, DWORD PTR DS:[EAX]	
0040163C	. 8B09	MOV ECX, DWORD PTR DS:[ECX]	
0040163E	. 894D E0	MOV DWORD PTR SS:[EBP-20], ECX	
00401641	. 50	PUSH EAX	
00401642	. 51	PUSH ECX	
00401643	. E8 59010000	CALL Malware_.004017A1	
00401648	. 50	POP ECX	
00401649	. 59	POP ECX	
0040164A	. C3	RETN	
0040164B	. 8B	DB 8B	

ECX=1DB10106

Malware_.<ModuleEntryPoint>+38

Registers (FPU)

EAX	1DB10106
ECX	1DB10106
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015AF
C 0	ES 002B
P 1	CS 002B
A 0	SS 002B
Z 1	DS 002B
S 0	FS 0053
T 0	GS 002B
D 0	
O 0	LastErr
EFL	00010246
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 Cor
FCW	027F Pre

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Options Window Help

LEMTWHC/KBR...S

Address	Disassembly	Comment
00401594	. 83EC 10	SUB ESP,10
00401597	. 53	PUSH EBX
00401598	. 57	PUSH EDI
00401599	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
0040159A	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion
0040159D	. 33D2	XOR EDX,EDX
004015A3	. 8A04	MOV DL,AH
004015A5	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX
004015A7	. 8BC8	MOV ECX,EAX
004015AD	. 81E1 FF000000	AND ECX,0FF
004015B7	. 8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX
004015B8	. C1E1 08	SHL ECX,8
004015BE	. 03CA	ADD ECX,EDX
004015C0	. 8900 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
004015DA	. 6A 1C	PUSH 1C
004015DC	. E8 9A000000	CALL Malware_.0040167B
004015E1	. 59	POP ECX
004015E2	. 8365 FC 00	AND DWORD PTR SS:[EBP-4],0
004015E6	. E8 72070000	CALL Malware_.00401D5D
004015EB	. FF15 2C404000	CALL DWORD PTR DS:[<&KERNEL32.GetComm
004015F1	. A3 D8574000	MOV DWORD PTR DS:[4057D8],EAX
004015F6	. E8 30060000	CALL Malware_.00401C2B
004015FB	. A3 B0524000	MOV DWORD PTR DS:[4052B0],EAX
00401600	. E8 D9030000	CALL Malware_.004019DE
00401605	. E8 1B030000	CALL Malware_.00401925
0040160A	. E8 90000000	CALL Malware_.0040169F
0040160F	. A1 E4524000	MOV EAX,DWORD PTR DS:[4052E4]
00401614	. A3 E8524000	MOV DWORD PTR DS:[4052E8],EAX
00401619	. 50	PUSH EAX
0040161A	. FF35 DC524000	PUSH DWORD PTR DS:[4052DC]
00401620	. FF35 D8524000	PUSH DWORD PTR DS:[4052D8]
00401626	. E8 F0FAFFFF	CALL Malware_.00401128
0040162B	. 83C4 0C	ADD ESP,0C
0040162E	. 8945 E4	MOV DWORD PTR SS:[EBP-1C],EAX
00401631	. 50	PUSH EAX
00401632	. E8 95000000	CALL Malware_.004016CC
00401637	. 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]
0040163A	. 8B08	MOV ECX,DWORD PTR DS:[EAX]
0040163C	. 8B09	MOV ECX,DWORD PTR DS:[ECX]
0040163E	. 894D E0	MOV DWORD PTR SS:[EBP-20],ECX
00401641	. 50	PUSH EAX
00401642	. 51	PUSH ECX
00401643	. E8 59010000	CALL Malware_.004017A1
00401648	. 59	POP ECX
00401649	. 59	POP ECX
0040164A	. C3	RETN
0040164B	. 5B	DB 5B

Registers (F)

Register	Value
EAX	10B10106
ECX	00000006
EDX	00000001
EBX	7EFD0000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000
EDI	00000000
EIP	004015B5
C 0	ES 002B
P 1	CS 0023
A 0	SS 002B
Z 0	DS 002B
S 0	FS 0053
T 0	GS 002B
D 0	
O 0	LastErr
EFL	00010206
ST0	empty 0.
ST1	empty 0.
ST2	empty 0.
ST3	empty 0.
ST4	empty 0.
ST5	empty 0.
ST6	empty 0.
ST7	empty 0.
FST	0000 Co
FCW	027F Pr

ECX=00000006
DS:[004052D0]=00000000
Malware_.<ModuleEntryPoint>+3E