



03/04/2024

OllyDBG

Prepared by:
Manuel Buonanno

Organized by:



Indice

1) Traccia.....	3
2) Punto 1.....	4
3) Punto 2.3.4.5.....	5
4) Punto 6.7.8.....	6
5) Bonus.....	7

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).
- BONUS: spiegare a grandi linee il funzionamento del malware.

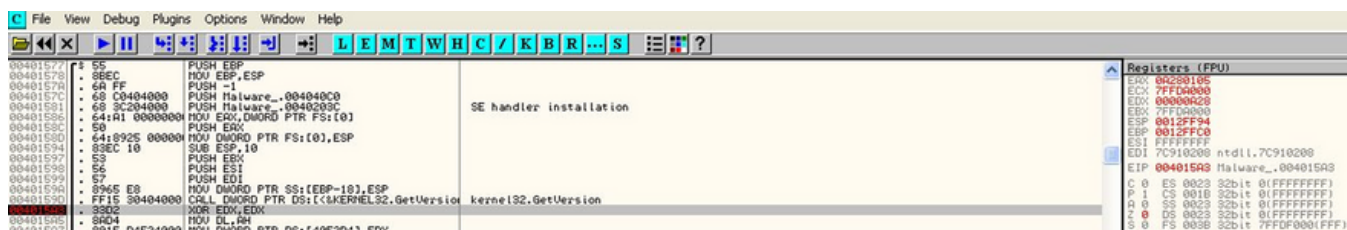
Punto 1

00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	pStartupInfo
00401059	. 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	CommandLine = "cmd"
00401067	. 68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	. 6A 00	PUSH 0	CreateProcessA
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	Timeout = INFINITE
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	hObject
00401077	. 6A FF	PUSH -1	WaitForSingleObject
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	
0040107C	. 51	PUSH ECX	
0040107D	. FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSi	
00401083	. 33C0	XOR EAX,EAX	
00401085	. 8BE5	MOV ESP,EBP	
00401087	. 5D	POP EBP	
00401089	. C3	RETN	

Il valore del parametro è «CMD» ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo 00401067.

Punto 2.3.4.5

Una volta configurato il breakpoint, clicchiamo su «play», il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è «00000A28».



The screenshot shows a debugger window with the following assembly code and registers:

Address	Disassembly	Comment
00401577	55	PUSH EBP
00401578	5B	MOV EBP, ESP
00401579	6A FF	PUSH -1
0040157C	68 00404000	PUSH Malware_.00404000
00401581	68 3C204000	PUSH Malware_.0040203C
00401586	64:R1 00000000	MOV EDX, DWORD PTR FS:[0]
0040158C	50	PUSH EDI
0040158D	64:8925 000000	MOV DWORD PTR FS:[0], ESP
00401594	83EC 10	SUB ESP, 10
00401597	53	PUSH EDI
00401598	56	PUSH ESI
00401599	57	PUSH EDI
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-10], ESP
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion
004015A0	33D2	XOR EDX, EDX
004015A5	8D04	MOV DL, 04
004015A7	8D1C 00000000	MOV DWORD PTR DS:[0], EDI

Registers (FPU):

Register	Value
EAX	00200105
ECX	7FFD0000
EDX	00000A28
EBX	7FFD0000
ESP	0012FF34
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015A3 Malware_.004015A3
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
D 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)
B 0	GS 0000 32bit 7FFDF000(FFF)

Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà 0.



The screenshot shows the same debugger window after the instruction XOR EDX,EDX has been executed. The value of the EDX register has changed from 00000A28 to 00000000.

Address	Disassembly	Comment
00401577	55	PUSH EBP
00401578	5B	MOV EBP, ESP
00401579	6A FF	PUSH -1
0040157C	68 00404000	PUSH Malware_.00404000
00401581	68 3C204000	PUSH Malware_.0040203C
00401586	64:R1 00000000	MOV EDX, DWORD PTR FS:[0]
0040158C	50	PUSH EDI
0040158D	64:8925 000000	MOV DWORD PTR FS:[0], ESP
00401594	83EC 10	SUB ESP, 10
00401597	53	PUSH EDI
00401598	56	PUSH ESI
00401599	57	PUSH EDI
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-10], ESP
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion
004015A0	33D2	XOR EDX, EDX
004015A5	8D04	MOV DL, 04
004015A7	8D1C 00000000	MOV DWORD PTR DS:[0], EDI

Registers (FPU):

Register	Value
EAX	00200105
ECX	7FFD0000
EDX	00000000
EBX	7FFD0000
ESP	0012FF34
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015A5 Malware_.004015A5
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
D 0	SS 0023 32bit 0(FFFFFFFF)
Z 1	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFDF000(FFF)
B 0	GS 0000 32bit 7FFDF000(FFF)

Punto 6.7.8

Configuriamo il secondo breakpoint. Il valore del registro ECX è «0A280105».

Registers (FPU)

EAX	0A280105
ECX	0A280105
EDX	00000001
EBX	77FD0000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910
EIP	004015AF Malware_.00
C 0	ES 0023 32bit 0(FFF
P 1	CS 001B 32bit 0(FFF
A 0	SS 0023 32bit 0(FFF
Z 1	OS 0023 32bit 0(FFF
S 0	FS 003B 32bit 77FDF
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_INVAL
EFL	00000246 (NO, NB, E, BE
ST0	empty -UNORM BCBC 01
ST1	empty -UNORM 0069 00
ST2	empty 0.0

Dopo lo step-into il valore del registro ECX è stato modificato in «00000005» in quanto è stata eseguita l'istruzione AND ECX, FF.

Registers (FPU)

EAX	0A280105
ECX	00000005
EDX	00000001
EBX	77FD0000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	00401585 Malware_.00401585
C 0	ES 0023 32bit 0(FFFFFFFF
P 1	CS 001B 32bit 0(FFFFFFFF
A 0	SS 0023 32bit 0(FFFFFFFF
Z 0	OS 0023 32bit 0(FFFFFFFF
S 0	FS 003B 32bit 77FDF000(FFF
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_INVALID_HANDLE (000
EFL	00000206 (NO, NB, NE, A, NS, PE, GE, O)
ST0	empty -UNORM BCBC 01050104 005C000
ST1	empty -UNORM 0069 006E0069 002E000
ST2	empty 0.0
ST3	empty 0.0
ST4	empty 0.0
ST5	empty 0.0
ST6	empty 0.0
ST7	empty 0.0

Nel dettaglio, l'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa portiamo entrambi i valori in formato binario e poi eseguiamo l'AND logico tra i bit.

Esadecimale	Binario
0A280105	0000 1010 0010 1000 0000 0001 0000 0101
FF	0000 0000 0000 0000 0000 0000 1111 1111

Eseguendo l'AND logico tra i bit uno ad uno: 0000 0000 0000 0000 0000 0000 0101. Che in Esadecimale è 00000005. Ecco spiegato il valore di ECX dopo l'istruzione AND ECX, 0FF.

Bonus

Risalendo quindi all'hash tramite CFF Explorer e caricandolo su Virus Total per farlo analizzare, questo malware sembrerebbe un Trojan.