

SII/L3

Stefano Di Prospero

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: spiegate a grandi linee i funzionamento del malware

C CPU - main thread, module Malware_

00401044	. 8955 E0	MOV DWORD PTR SS:[EBP-20],EDX
00401047	. 8845 E0	MOV EAX,DWORD PTR SS:[EBP-20]
0040104A	. 8945 E8	MOV DWORD PTR SS:[EBP-18],EAX
0040104D	. 8840 E8	MOV ECX,DWORD PTR SS:[EBP-18]
00401050	. 8940 E4	MOV DWORD PTR SS:[EBP-1C],ECX
00401053	. 8055 F0	LEA EDX,DWORD PTR SS:[EBP-10]
00401056	. 52	PUSH EDX
00401057	. 8045 A8	LEA EAX,DWORD PTR SS:[EBP-58]
0040105A	. 50	PUSH EAX
0040105B	. 6A 00	PUSH 0
0040105D	. 6A 00	PUSH 0
0040105F	. 6A 00	PUSH 0
00401061	. 6A 01	PUSH 1
00401063	. 6A 00	PUSH 0
00401065	. 6A 00	PUSH 0
00401067	. 68 30504000	PUSH Malware_.00405030
0040106C	. C0 00	PUSH 0
0040106E	. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX
00401077	. 6A FF	PUSH -1
00401079	. 8840 F0	MOV ECX,DWORD PTR SS:[EBP-10]
0040107C	. 51	PUSH ECX
0040107D	. FF15 00404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSingleObject]
00401083	. 33C0	XOR EAX,EAX
00401085	. 8BE5	MOV ESP,EBP
00401087	. 50	POP EBP
00401088	. C3	RETN
00401089	. 55	PUSH EBP
0040108A	. 8BEC	MOV EBP,ESP
0040108C	. 81EC 08010000	SUB ESP,108
00401092	. F7	PUSH EDI

Il valore che il parametro passa sullo stack è “cmd”

C CPU - main thread, module Malware_

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 00000001	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 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	8900 00524000	MOU DWORD PTR DS:[4052D001] ECX

Registers (FPU)

EDX	00001DB1
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
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 7EFDD000(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)

PRIMA

Arrivando all'indirizzo **004015A3**, prima che quest'ultimo esegua il suo comando,
il valore di EDX è **00001DB1**

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 00000001	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 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

Registers (FPU)

EDX	00000000
EBX	7EFDE000
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 7EFDD000(FFF)
T	0 GS 002B 32bit 0(FFFFFFFF)
D	0
O	0 LastErr ERROR_SUCCESS (00000000)
EFL	00000214 (NO,NB,NE,A,NS,PE,GE,G)

DOPO

Dopo lo step-into e quindi l'esecuzione del comando **XOR EDX, EDX**, il valore di EDX sarà **0**

L'azzeramento del valore è dato dallo XOR che quando fa il confronto tra due variabili le inizializza a 0

C CPU - main thread, module Malware_

```

00401573 > FC      CLD
00401574 . SF      POP EDI
00401575 . 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
0040157D . 68 3C204000 PUSH Malware_.0040203C
00401581 . 68 A1 00000000 MOV EAX,DWORD PTR FS:[0]
00401586 . 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
0040159D FF15 30404000 CALL DWORD PTR DS:[&KERNEL32.GetVersion]
004015A3 004015AF kernel32.GetVersion
004015A5 . 8AD4   MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015A8 . 8BC8   MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8

```

SE handler installation

	EAX	ECX	EDX	EBX	ESP	EBP	ESI	EDI	EIP	LastError	EFL	ST0	ST1	ST2	ST3	ST4	
	1DB10106	1DB10106	00000001	7EFDE000	0018FF5C	0018FF88	00000000	00000000	004015AF	ERROR_SUCCESS	00000246	empty 0.0					
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	7EFDD000(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

PRIMA

Il valore di ECX prima di arrivare all'indirizzo 004015AF è 1DB10106

DOPO

```

00401573 > FC      CLD
00401574 . SF      POP EDI
00401575 . 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
0040157D . 68 3C204000 PUSH Malware_.0040203C
00401581 . 68 A1 00000000 MOV EAX,DWORD PTR FS:[0]
00401586 . 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
0040159D FF15 30404000 CALL DWORD PTR DS:[&KERNEL32.GetVersion]
004015A3 004015B5 kernel32.GetVersion
004015A5 . 8AD4   MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015A8 . 8BC8   MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA   ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC1],ECX

```

SE handler installation

	EAX	ECX	EDX	EBX	ESP	EBP	ESI	EDI	EIP	LastError	EFL	ST0	ST1	ST2	ST3	ST4	
	1DB10106	00000006	00000001	7EFDE000	0018FF5C	0018FF88	00000000	00000000	004015B5	ERROR_SUCCESS	00000000	P	1	CS	0023	32bit	0(FFFFFFFF)
Z	0	DS	002B	32bit	0(FFFFFFFF)	S	0	FS	0053	32bit	7EFDD000(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

Dopo lo step-into il valore diventa 00000006

Considerazione Finale

Dal tipo di librerie e registri che si notano dall'analisi del malware, esso sembra cerchi di ottenere informazioni su sistema, inoltre agisce sui registri per manipolare l'esecuzione del malware e replicarsi.

Manipolazione di memoria e registri, chiamate a funzioni di sistema, parti di copia e spostamento dati.
Il malware potrebbe essere un Trojan