

Pratica S11/L3

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

1.Valore del parametro «CommanLine»

Il valore del parametro è «cmd», cioè il Prompt dei comandi di Widnows

00401063	. 0A 00	PUSH 0	pProcessSecurity = NULL
00401065	. 6A 00	PUSH 0	pProcessSecurity = 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

2.All'indirizzo 004015A3 qual è il valore del registro EDX?

Inserito un breakpoint all'indirizzo **004015A3**

0040157H	. 8763 E0	MOV DWORD PTR SS:[EBP+10],E3F	
0040159D	. FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	ke
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	

Il valore di EDX è **00001DB1**

```
ECX 7EFDE000
EDX 00001DB1
EBX 7EFDE000
```

3.Eseguire uno «step-into». Qual è ora il valore del registro EDX?

Adesso il valore di EDX è **00000000**

0040157D	. FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	
004015A3	. 33D2	XOR EDX,EDX	
004015A5	. 8AD4	MOV DL,AH	
004015C7	. 8915 04524000	MOV DWORD PTR DS:[4052041],EDX	

```
ECX 7EFDE000
EDX 00000000
EBX 7EFDE000
```

4.Motivare la risposta.

Dopo aver inserito il breakpoint all'indirizzo **004015A3**, cliccando su Play il programma si ferma sull'istruzione **XOR EDX, EDX** indicato il valore di **EDX**.

5.Che istruzione è stata eseguita?

Dopo lo «step-into» viene eseguito **XOR EDX, EDX** azzerando il valore di EDX portandolo a 0

6.All'indirizzo 004015AF qual è il valore del registro ECX?

Inserito un breakpoint all'indirizzo **004015AF**

004015AD	. 8BC8	MOV ECX,EAX
004015AF	. 81E1 FF000000	AND ECX,0FF
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX
004015BB	. C1F1 00	SHI ECX,0

Il valore di ECX è **0DB10106**

```
EAX 1DB10106
ECX 1DB10106
EDX 00000001
EBX 77F14332
```

7.Eeguire uno «step-into». Qual è ora il valore di ECX?

Adesso il valore è **00000006**

```
EAX 1DB10106
ECX 00000006
EDX 00000001
EBX 77F14332
```

8.Spiegare quale istruzione è stata eseguita.

L'istruzione eseguita è **AND ECX, 0FF**

Bonus: Spiegare a grandi linee il funzionamento del malware

Il file Malware_U3_W3_L3 è un Trojan Horse (info Virus Total).

Utilizzare il Prompt dei Comandi di Windows per poter creare un file all'interno del disco in modo, anche in un secondo momento, per prenderne il controllo.