

S11L3,

BENVENUTI LUIGI

### 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**.

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?
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?
3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
4. BONUS: spiegare a grandi linee il funzionamento del malware

### 1 – Valore “CommandLine”

00401061	. 6H 01	PUSH 1	InheritHandles = TRUE
00401063	. 6A 00	PUSH 0	pThreadSecurity = 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

Il valore di CommandLine passato sullo stack è quello descritto all'indirizzo 00401067, ovvero “cmd”, la command line di Windows.

### 2 – Breakpoint software a 004015A3

0040158D	. 64:8925 00000	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	. 8A04	MOV DL,AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	

EDX=00001DB1

Malware\_.<ModuleEntryPoint>+2C

Per inserire un software breakpoint basta cliccare sull'indirizzo di memoria desiderato e selezionare nel menù a tendina breakpoint > toggle.

Il valore di EDX è 00001DB1, sottolineato in figura in rosso.

Dopo aver eseguito lo step into, notiamo che il valore del registro passa a 00000000, questo perché l'operatore logico XOR fra un elemento e sé stesso inizializza il registro a zero.

### 3 - Breakpoint software a 004015AF

004015A7	. 8715 04524000	MOV DWORD PTR DS:[4052D4],EAX	
004015A9	. 8BC8	MOV ECX,EAX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 8900 00524000	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	
ECX=1DB10106			
Malware_.<ModuleEntryPoint>+38			

Il valore di ECX è 1DB10106, sottolineato in figura in rosso.

Dopo aver eseguito lo step into, notiamo che il valore del registro passa a 00000006, come risultato dell'operazione logica AND fra il contenuto del registro ECX e il valore 0FF.

### 4 – Comportamento generale malware

Dalle API consultate dal malware e dalle funzioni chiamate, possiamo presumere che il malware sia un downloader.