# Pratica S11/L3 Giaimo Rosario

#### Traccia:

Fate riferimento al malware: Malware\_U3\_W3\_L3, presente all'interno della cartella Esercizio\_Pratico\_U3\_W3\_L3sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- All'indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpointsoftware 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 breakpointall'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

## **Svolgimento**

 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)

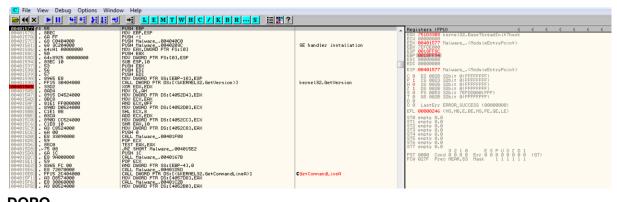
0040105F	6A 00	PUSH 0	
00401061	6A 01	PUSH 1	
00401063		PUSH 0	
00401065		PUSH 0	
			00077 ##
			HSUII "CMd"
		PUSH 0	
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	kernel32.CreateProcessA
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14].EAX	
00401077	60 FF		
			L
			kernel32.WaltrorSingleUbject
00401089	8BE5	MOV ESP.EBP	
00401087	50	POP ERP	
00401957 80401965 9040107 9040107 9040107 9040107 9040107 9040108 9040108 9040108 9040108 9040108 9040108	68 30504000 6A 00 FF15 04404000 8945 EC 6A FF 8840 F0 51 51 00404000 3350 8EE5 5D C3 8EC 8EC	PÜSH Malware00405030 PUSH 0	

Il valore del parametro è "CMD"

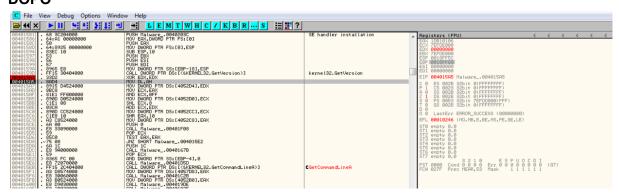
• Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

Il valore del registro EDX è 00401577

#### **PRIMA**

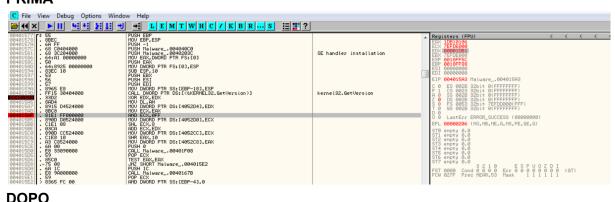


#### **DOPO**

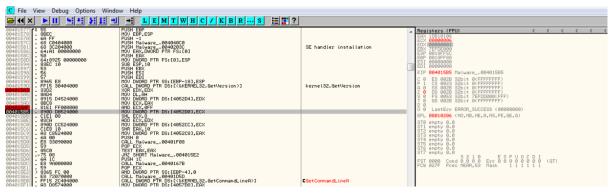


• Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7)Spiegate quale istruzione è stata eseguita (8).

#### **PRIMA**



### **DOPO**



BONUS: spiegare a grandi linee il funzionamento del malware

Dall'analisi che ho effettuato la minaccia in questione potrebbe essere un Trojan, ma è probabile che si tratti di uno Spyware.