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.

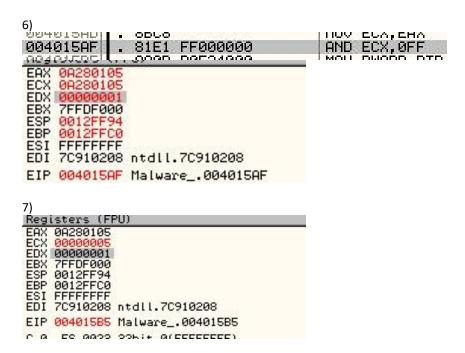
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto 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

2)
004015A3

3) EAX 0A280105 ECX 7FFD4000 EDX 04000000 EBX 7FFD4000 EBX 7FFD4000 ESP 0012FF94 EBP 0012FF00 ESI FFFFFFF EDI 7C910208 ntdll.7C910208 EIP 004015A5 Malware_.004015A5

4/5) XOR fa resettare il valore delle variabili essendo la stessa, XOR = NOT OR, quindi EDX essendo uguale EDX, ritorna 0.

3



8) AND fa passare entrambi i valori se son veri, compiono con la funzione e riporta 1.