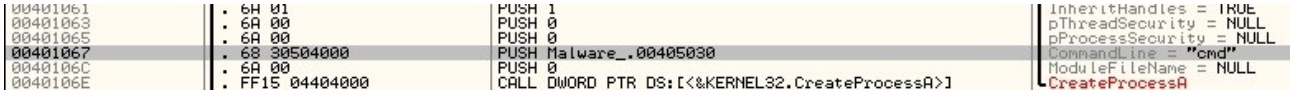
Esercizio settimana 11 lezione 3 Daniele D'Esposito

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.

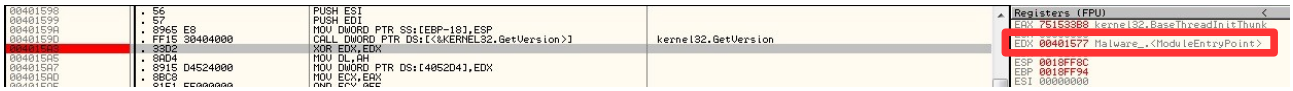
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo **stack**? **(1)**
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? **(2)** Eseguite a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

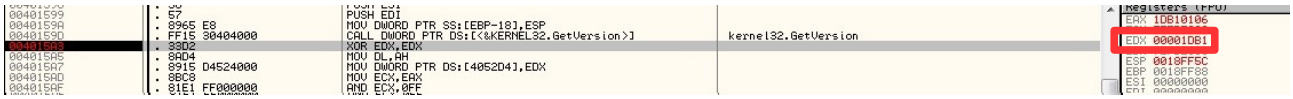


Come si vede dall'immagine, il valore che viene passato nella riga **00401067** dal comando **PUSH** e che corrisponde al parametro **CommandLine** della funzione **CreateProcessA** e' **Malware_.00405030**

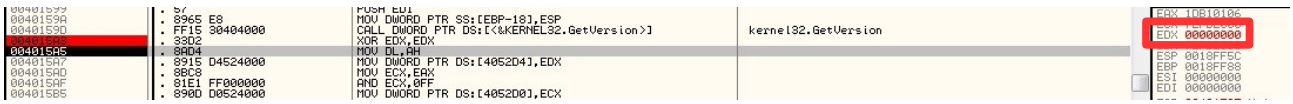
-2, 3, 4, 5



Come si vede dall'immagine, il valore che si trova nel registro **EDX** prima di avviare il programma dall'entry point e' proprio la riga di entry point



Dopo aver creato il **break point** alla riga **004015A3** ed aver avviato il malware, il valore del registro **EDX** cambia in **00001DB1**



Premendo il pulsante **step into**, il programma esegue solamente la riga successiva a dove si trova nel momento di pausa e nell'immagine si puo' vedere il risultato del comando della riga **004015A3**; il registro **EDX** ha cambiato valore in zero; l'operatore logico **XOR** produce in uscita il valore 1 se e solo se i valori in ingresso sono diversi tra loro; mettere 2 valori uguali all'ingresso di **XOR** e' un espediente per resettare il registro a zero in modo veloce.

A	B	A XOR B
0	0	0
0	1	1
1	0	1
1	1	0

-6, 7, 8

Il valore del registro **ECX** prima dell'esecuzione della riga **004015AF** e' **1DB10106**

Usando l'opzione **step into** si vede che e' cambiato in **00000006**; questo perche' l'operatore logico **AND** consegna in uscita un valore 1 solo quando entrambi i valori in ingresso sono 1; convertendo i valori della destinazione e della sorgente in binario e inserendoli nell'operatore logico si ottiene il valore sopra citato.

	ESADECIMALE	**BINARIO**
Destinazione:	**1DB10106 (ECX)**	**0 0 0 1 1 1 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0 0 1 1 0**
Sorgente:	**FF**	**0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1**
		AND
Risultato:	**6**	**0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 1 0**

A	**B**	**A AND B**
0	**0**	**0**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**