S11L3,

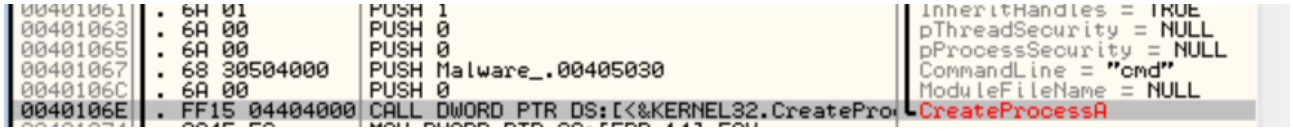
BENVENUTI LUIGI

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**.

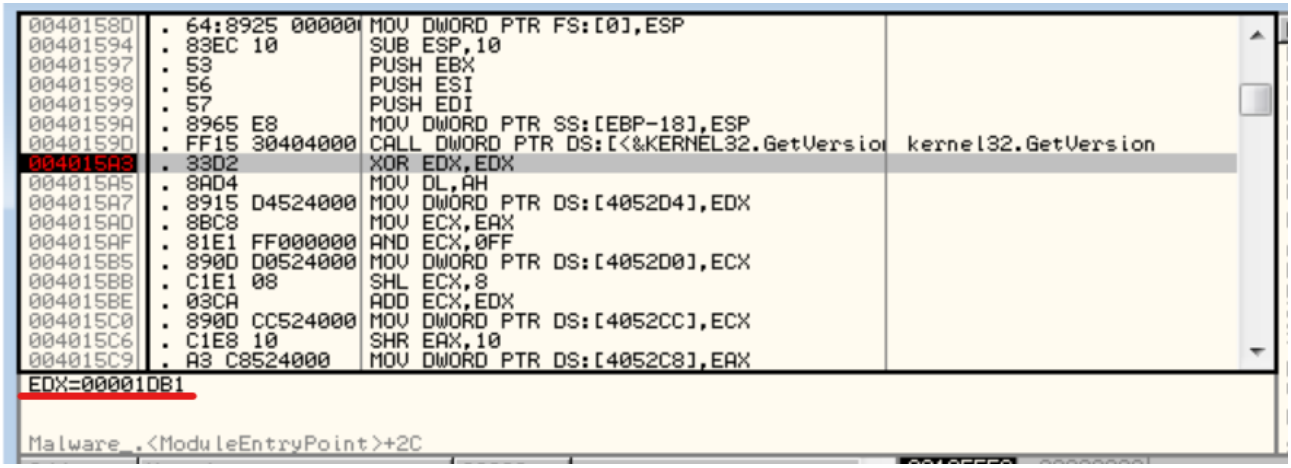
1. All'indirizzo **0040106E** il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
2. Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (Eseguite a questo punto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



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

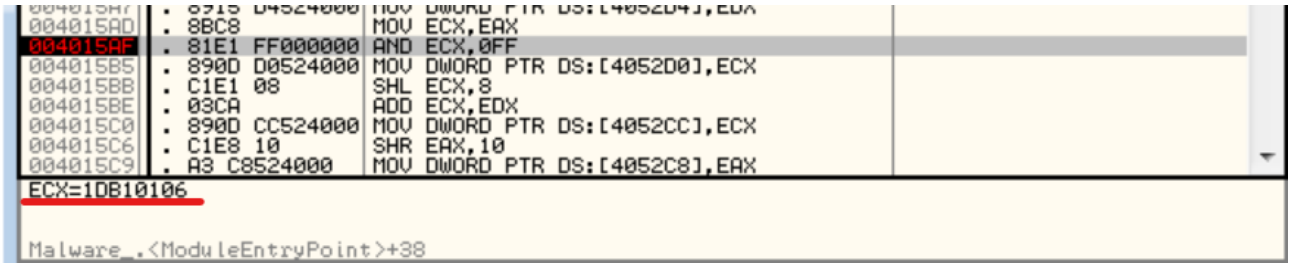


Per inserire un software breakpoint basta cliccare sull'indirizzo di memoria desiderato e selezionare nel menù a tendina breakpoint > toggle.

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



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.