S11L3

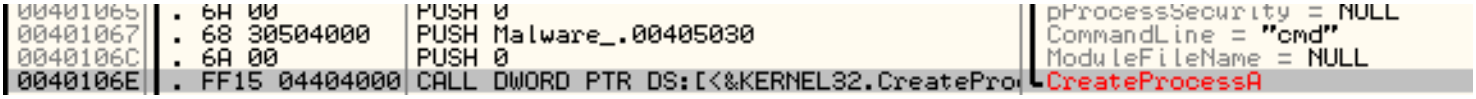
OllyDBG

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.

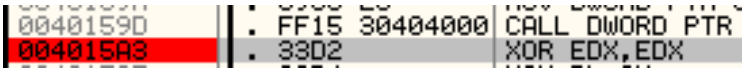
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto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

1)



Il valore del parametro «CommandLine» passato nello stack è "cmd"

2)



inseriamo il breakpoint e avviamo l'esecuzione del programma tramite OllyDBG

al breakpoint questo è il valore del registro EDX

3)

eseguendo un step-into il registro cambia il suo valore a 00000000, **(4,5)** per via dello XOR effettuato all'interno dell'istruzione che avevamo bloccato.

6)

al breakpoint questo è il valore del registro EDX

7)

eseguendo un step-into il registro cambia il suo valore a 00000005 **(8)** per via dell'AND effettuato all'interno dell'istruzione che avevamo bloccato.

(Bonus)
Ipotiziamo che il malware sia una backdoor, esso infatti crea un socket e aspetta una connessione in entrata