OllyDBG

Indice

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.

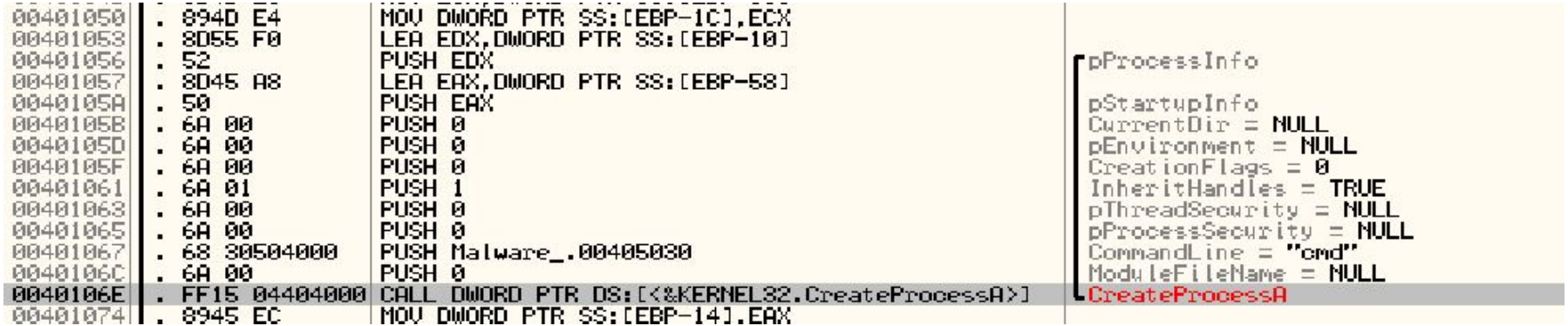
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo **stack**? **(1)**

- 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

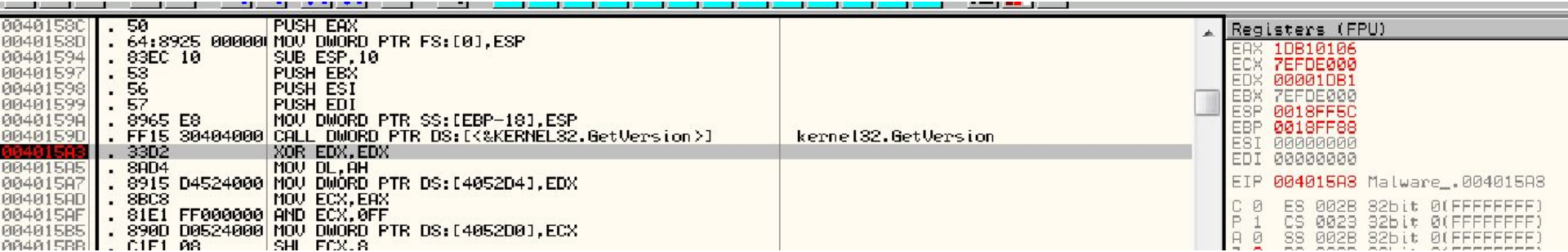
CreateProcess



Come si vede dalla figura qui sopra sulla riga 0040106E il malware crea il processo “A”. Sullo stack viene inserito il “CommanLine” dandogli il valore “cmd”.

Breakpoint software 1

Dopo aver impostato il breakpoint e avviato l'esecuzione con il pulsante "play", il programma si bloccherà all'istruzione XOR EDX,EDX. Prima dell'esecuzione di questa istruzione, il valore del registro è "00001DB1".

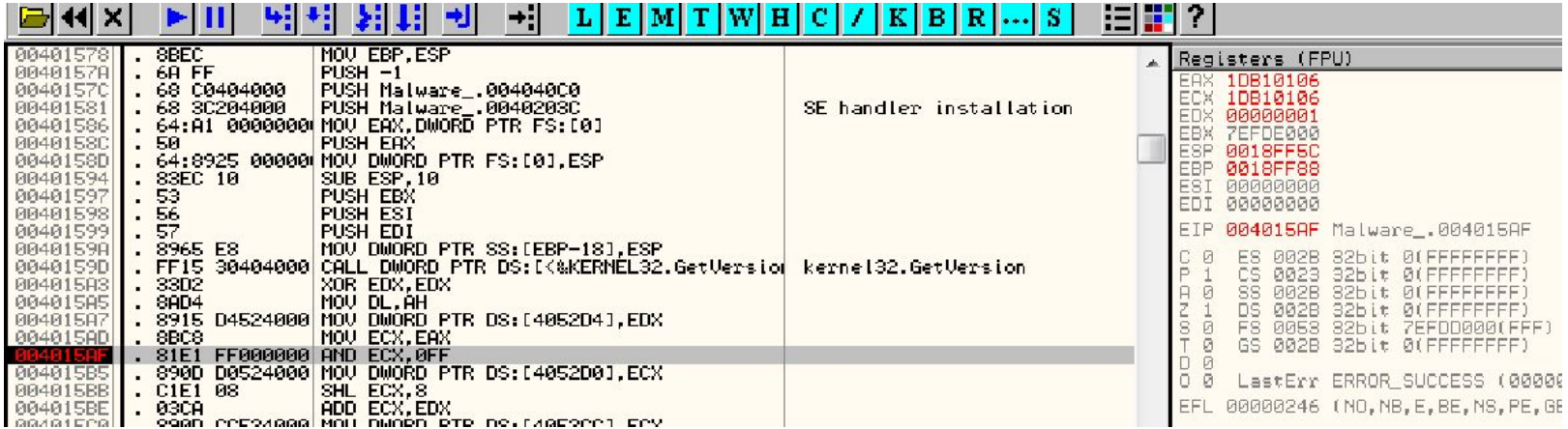


Step-into 1

Dopo aver eseguito lo step-into, l'istruzione XOR EDX,EDX viene eseguita, il che equivale fondamentalmente a inizializzare a zero una variabile. Quindi, dopo lo step-into, il valore di EDX sarà 0.

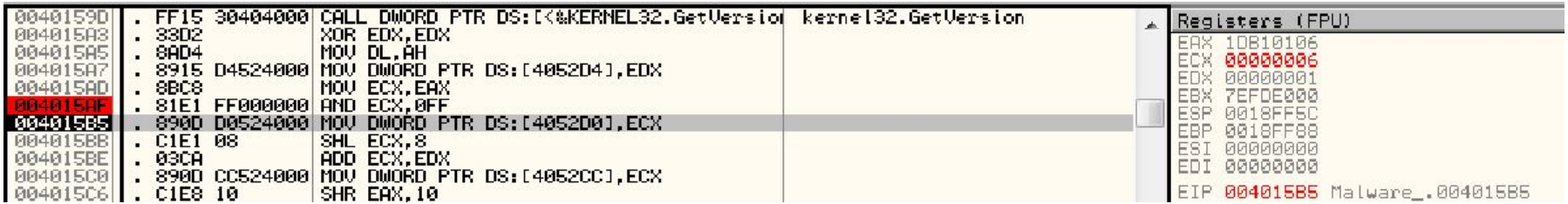
Breakpoint software 2

Come si vede in figura al breakpoint il valore di ECX è 1DB10106

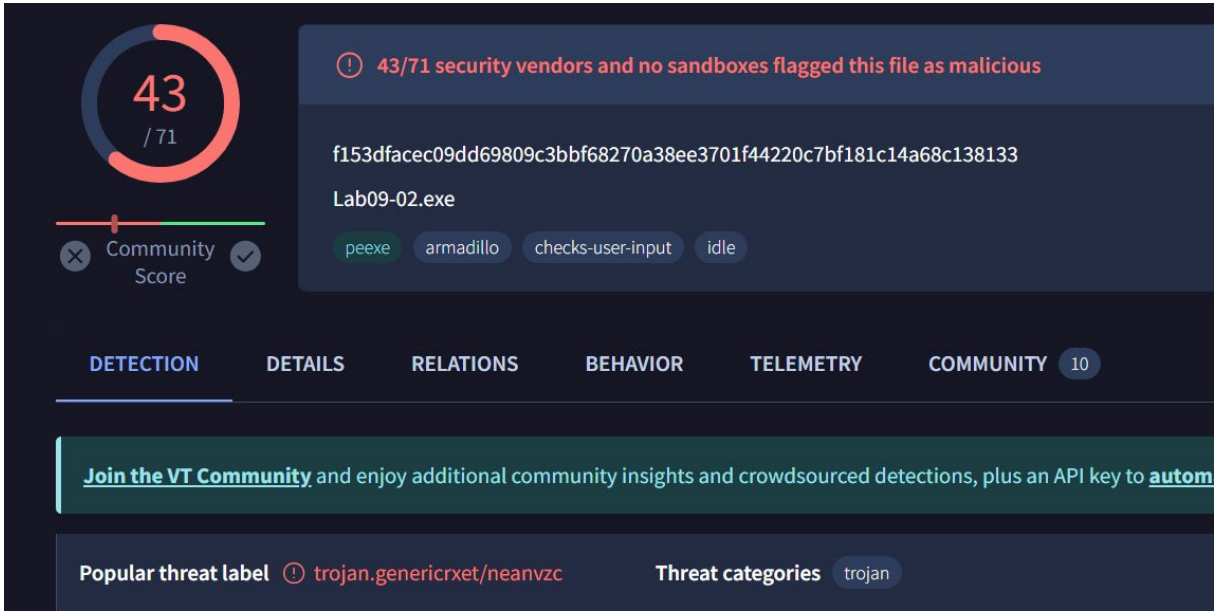


Step-into 2

Dopo aver eseguito lo step-into il valore di ECX cambia e diventa 00000006, perché viene eseguito il comando AND ECX, 0FF che significa che il valore 0FF (in binario =0000 0000 0000 0000 1111 1111) viene aggiunto con l'AND logico al valore ECX (in binario 1DB10106 diventa 0001 1101 1011 0001 0000 0001 0000 0110) con il risultato finale di ECX = 00000006.



Bonus



Dopo aver cercato l'hash del malware l'ho inserito sulla barra di ricerca di virus total e sembra essere un trojan

Grazie