Epicode

Malware Analysis
OllyDBG

Indice

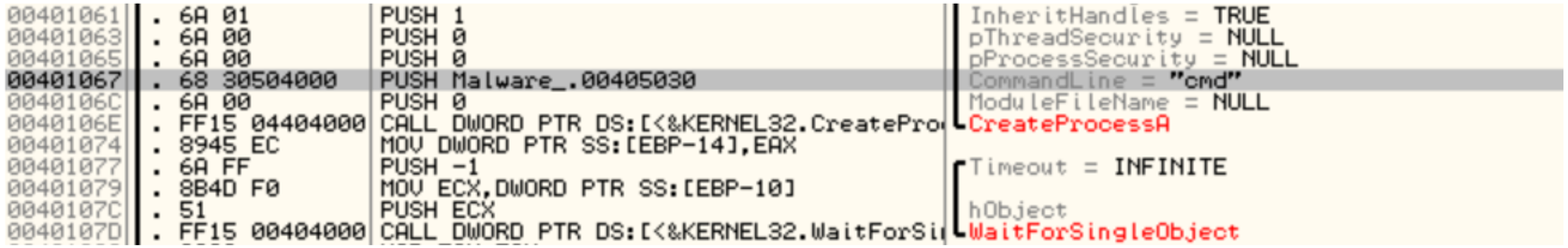
- Traccia
- Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
- 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?
- Inserite un secondo breakpointall’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
- BONUS: spiegare a grandi linee il funzionamento del malware

Traccia

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul 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

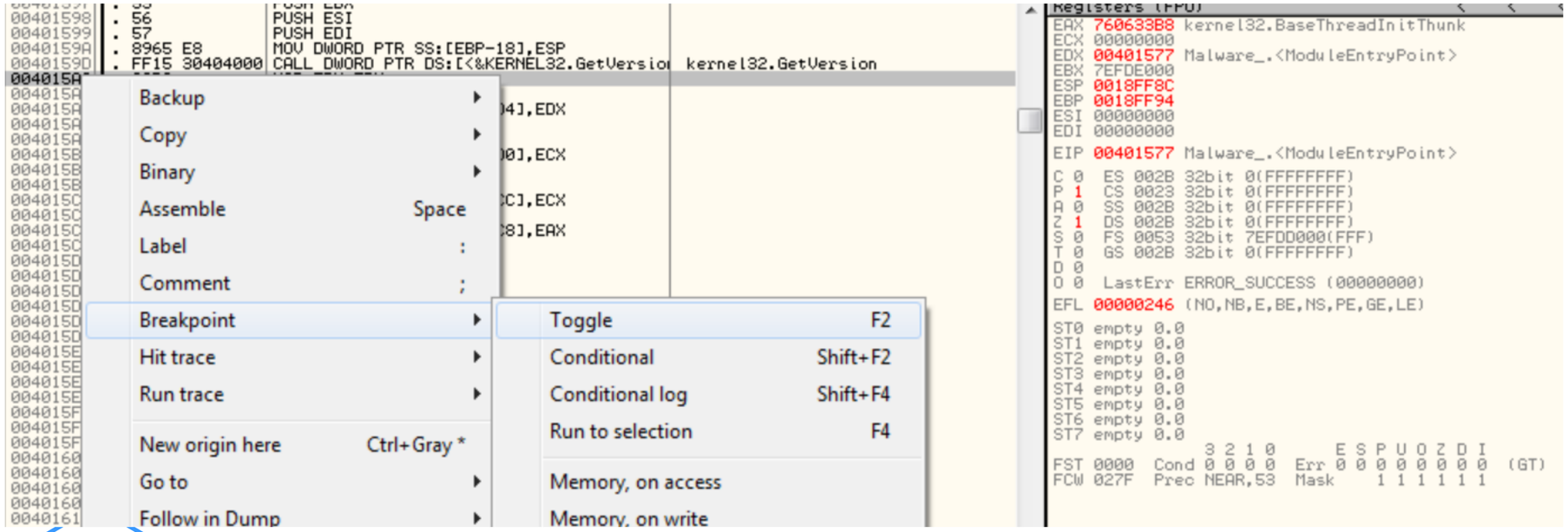
Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)



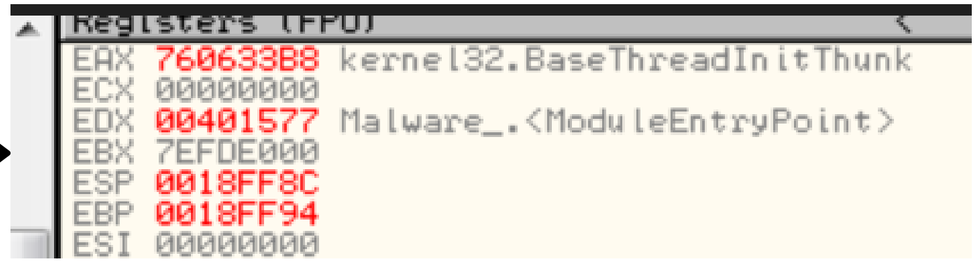
Il valore del paramento e “CMD”, dunque il prompt dei comandi di Windows, possiamo notarlo nella figura all’indirizzo 00401067

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?

Spostandoci all'allocazione di memoria 004015A3 andiamo ad impostare un breakpoint su una specifica istruzione nel programma.

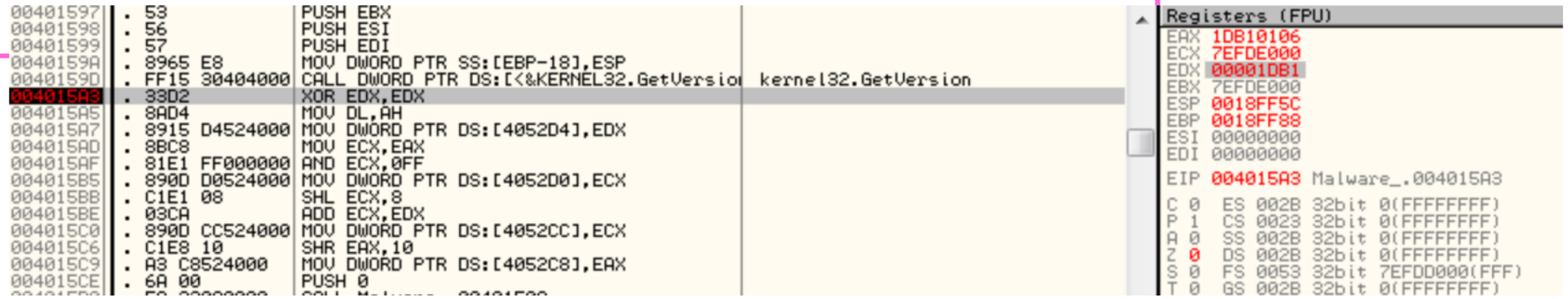


Inizialmente il registro EDX ha valore 00401577

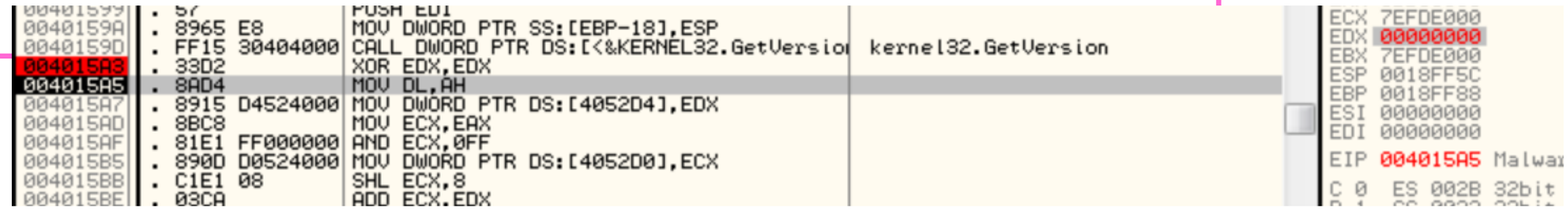


Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

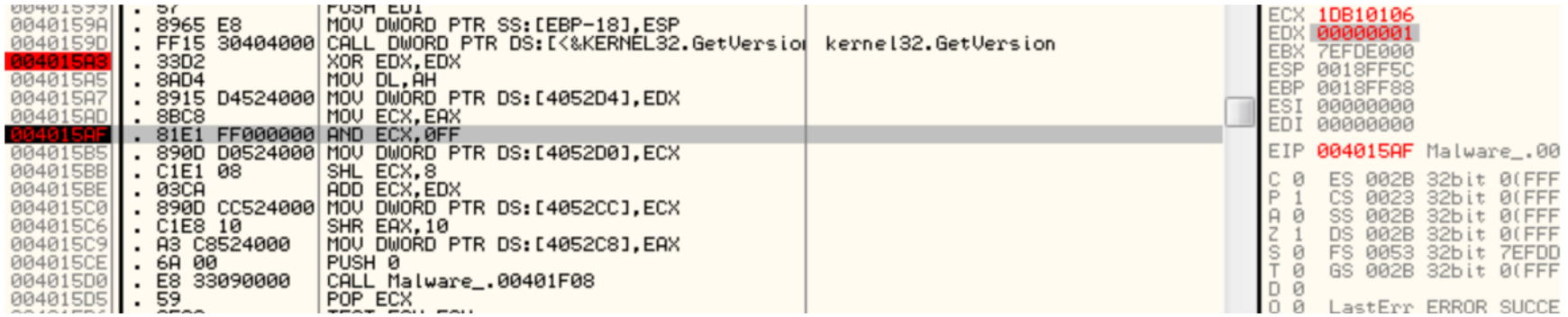
Interrompendo l'esecuzione del programma possiamo controllare il valore del registro EDX e verifichiamo che sembrerebbe essere 00001DB1. Continuiamo avviando l'esecuzione del programma cliccando sul tasto "play" nella barra degli strumenti. Attraverso la finestra "Registers FPU" è stato possibile verificare che il valore nel registro EDX sia rimasto lo stesso.



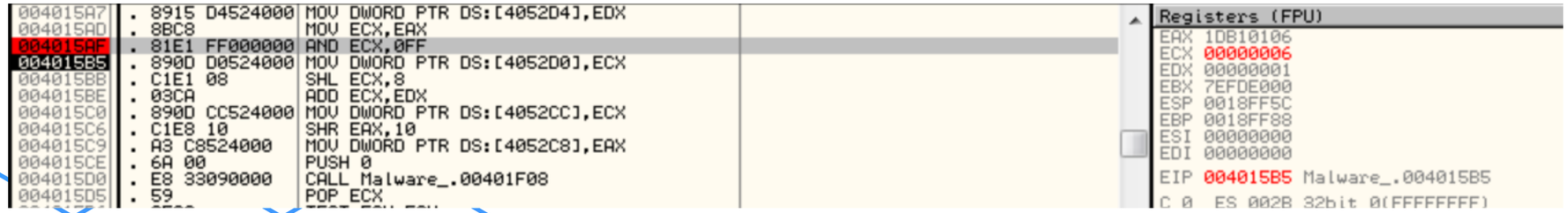
Utilizzando la funzione "Step-into" possiamo entrare nel codice della funzione in analisi. In questa fase possiamo notare che il valore del registro EDX è cambiato a 0. Questo cambiamento è dovuto all'operazione logica XOR nel codice, che restituisce sempre 0 quando applicata a due valori uguali. In questo caso, l'operazione XOR ha annullato il valore precedente di EDX, impostandolo a zero.



Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

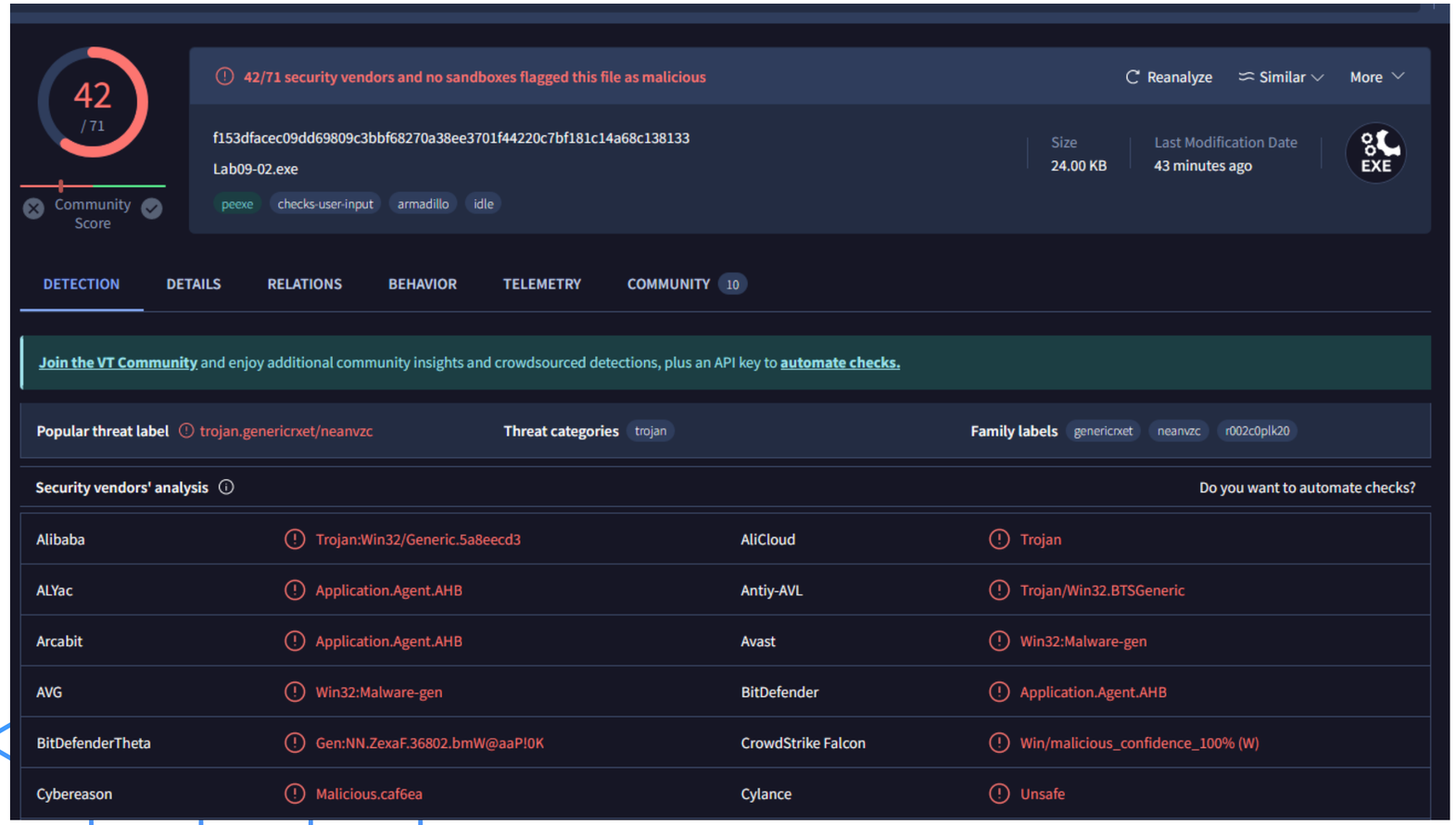


Configuriamo il secondo breakpoint all'indirizzo di memoria 004015AF.
Il valore del registro ECX è «1DB110106».



Dopo lo step-into il valore del registro ECX è stato modificato in «00000006» in quanto è stata eseguita l'istruzione AND ECX, FF.
Se l'operazione restituisce un risultato vero, il valore di ECX viene modificato

BONUS: spiegare a grandi linee il funzionamento del malware



Grazie a VirusTotal possiamo scoprire che il malware viene identificato molto probabilmente come trojan.