ANALISI DINAMICA AVANZATA

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.

(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 breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX?

(3) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX

(4) motivando la risposta

(5). Che istruzione è stata eseguita?

(6) Inserite un secondo breakpointall'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

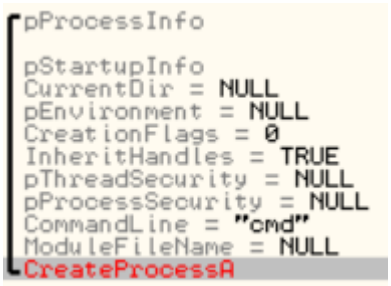
(7) Eseguite un step-into. Qual è ora il valore di ECX?

(8)Spiegate quale istruzione è stata eseguita.

(9) Che istruzione è stata eseguita?

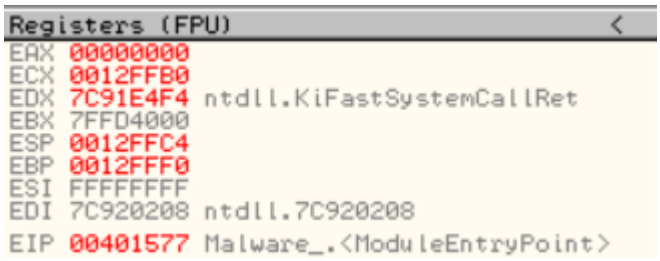
(10) BONUS: Capire di che malware si tratta

All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Aprendo il registro abbiamo visto il valore cmd «CommandLine» viene passato sullo stack



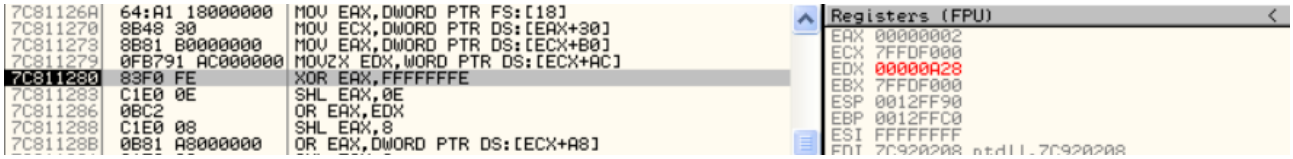
Cmd= command line

Dopo aver ricercato l'indirizzo richiesto (004015A3) clicchiamo per eseguire un breackpoint e spostandoci sui registri vediamo il valore del registro EDX.



EDX=7C91E4F4

Abbiamo ora eseguito uno step-into e visto che il valore di EDX è stato modificato.

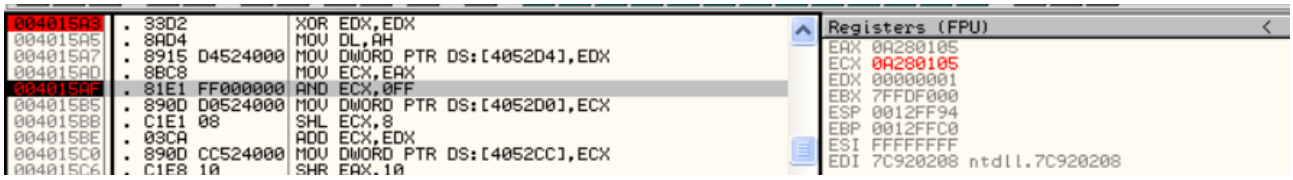


Il MOVZX copia il valore da un registro con dimensioni più piccole(8-16 bit) a uno di dimensioni superiori (16-32 bit).

Questo perché il comando MOVZX (nell'istruzione che vediamo nell'immagine) copia il valore di word dentro il registro EDX,

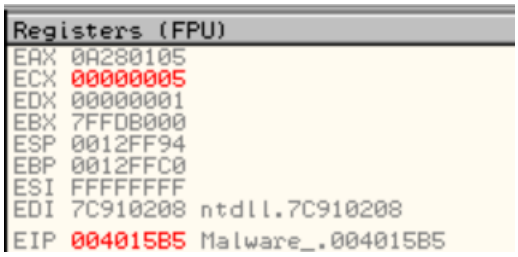
Proprio in quella riga di codice si vede infatti che il valore è stato modificato

Inserendo un secondo breakpoint all'indirizzo di memoria 004015AF. E spostandoci dalla parte dei registri vediamo il valore di ECX

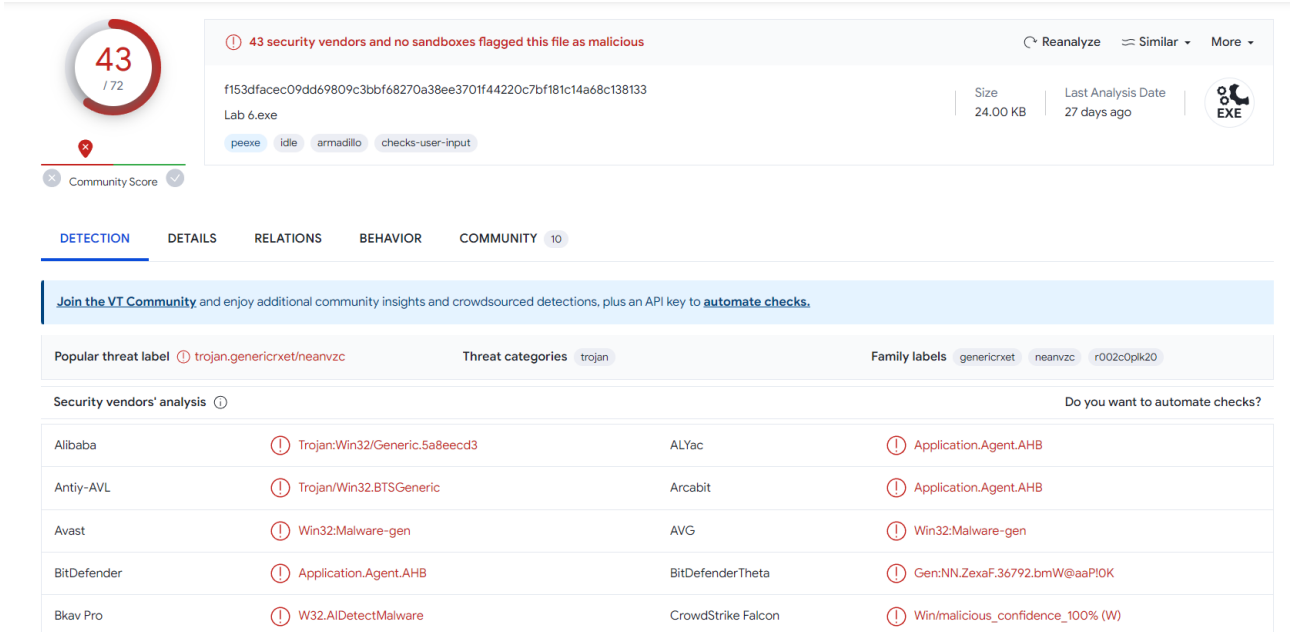


Eseguite un step-into notiamo che il valore di ECX cambia appena arriviamo all'istruzione AND ECX, 0FF

Notiamo che il valore verrà cambiato quando sarà eseguita l'istruzione AND con il registro ECX e il valore del numero esadecimale 0FF. il risultato ottenuto è il seguente



Infine è stato analizzato il malware utilizzando il tool cff explorer per ricavarci l'hash in formato md5 che abbiamo riportato su virus total e abbiamo avuto la seguente risposta alla scansione fatta dell'hash



Abbiamo dedotto quindi tramite virus total che il malware è un trojan