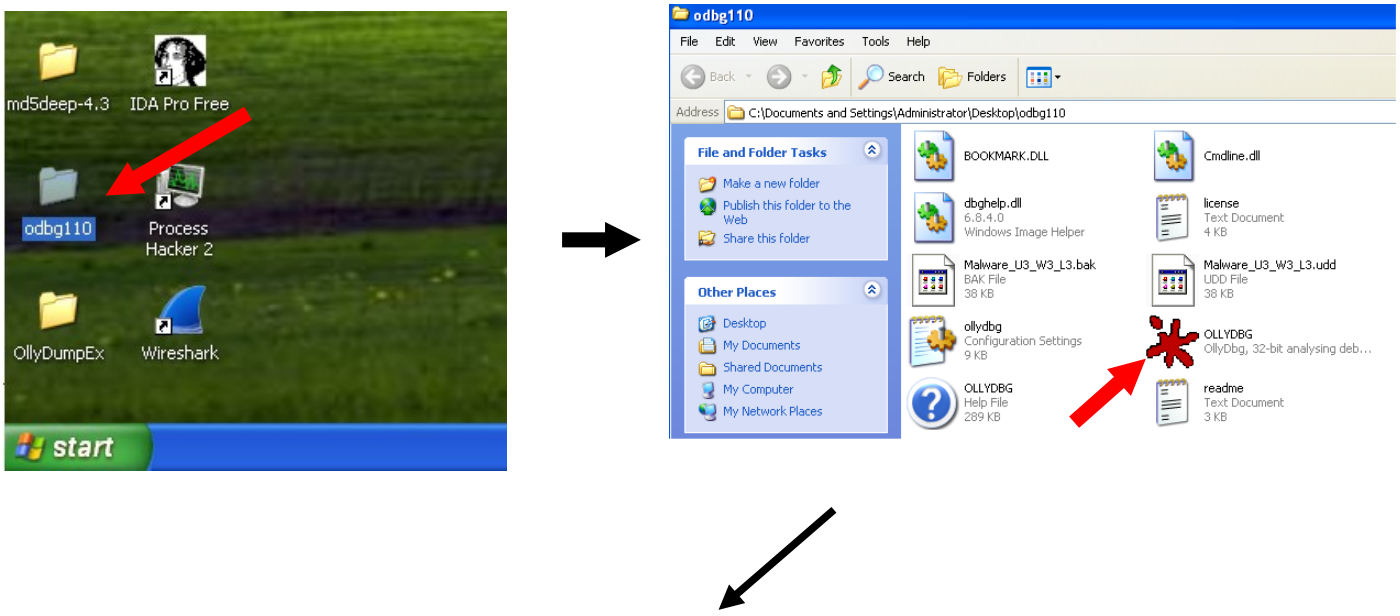
REPORT 18/01/2023 LORENZO SCORBAIOLI

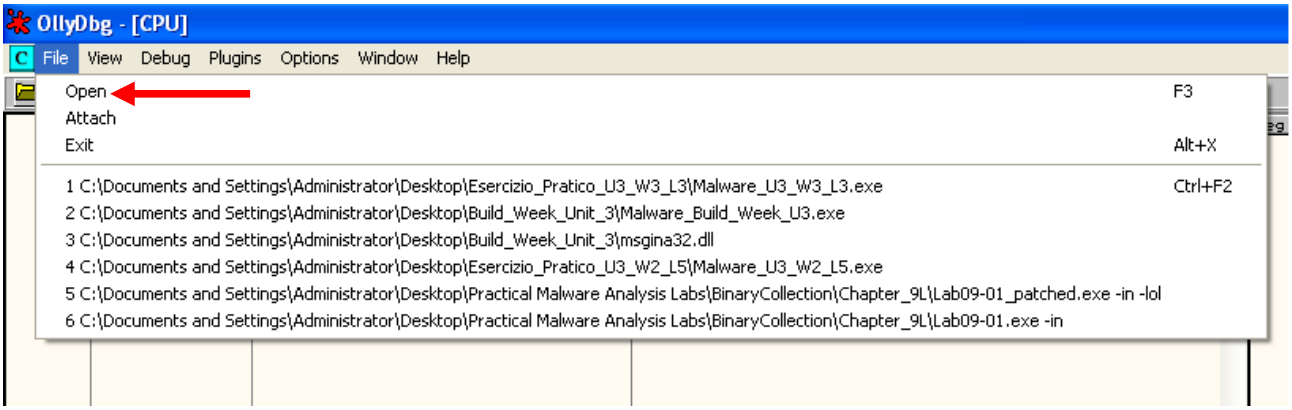
TASK:

In riferimento al malware “Malware_U3_W3_L3” rispondere ai seguenti quesiti utilizzando OllyDBG:

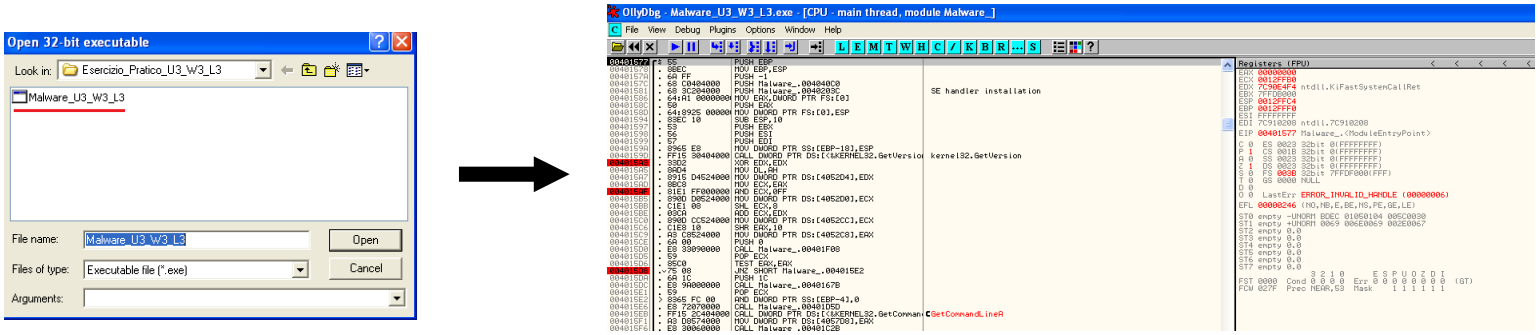
- All’indirizzo 0040106E viene effettuata una chiamata di funzione alla funzione <<CreateProcess>> . Qual è il valore del parametro <<CommandLine>> che viene passato sullo stack?(1)
- Inserire un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX? (2). Eseguite a questo punto uno <<step-into>>. Indicate qual è 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 uno <<step-into>>. Qual è il valore di ECX?(7) Spiegte uale istruzione è stata eseguita (8).
- Bonus: spiegare a grandi linee il funzionamento del malware (9)

Dopo avere avviato la macchina virtuale con sistema operativo Windows XP sono andato ad avviare il programma da usare per questa esercitazione: OllyDBG:



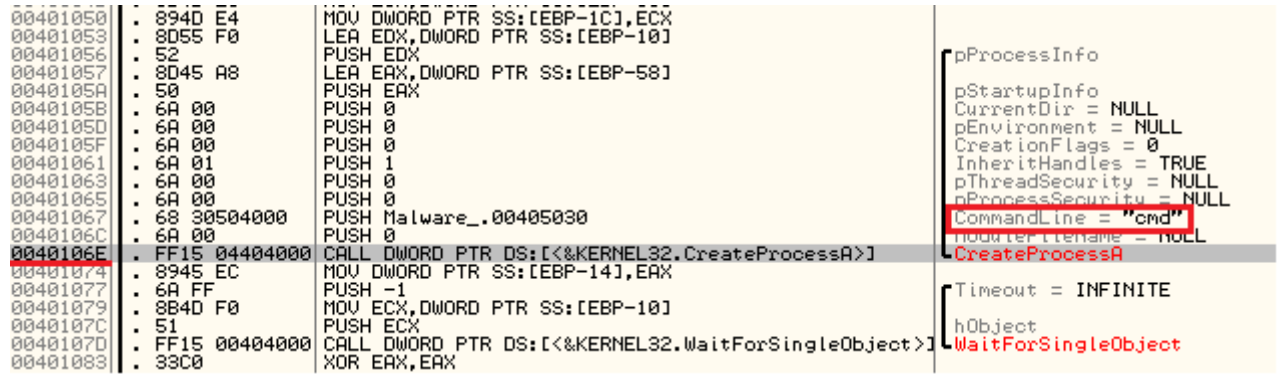


Ho selezionato dall’apposito menù il file da analizzare:



1)

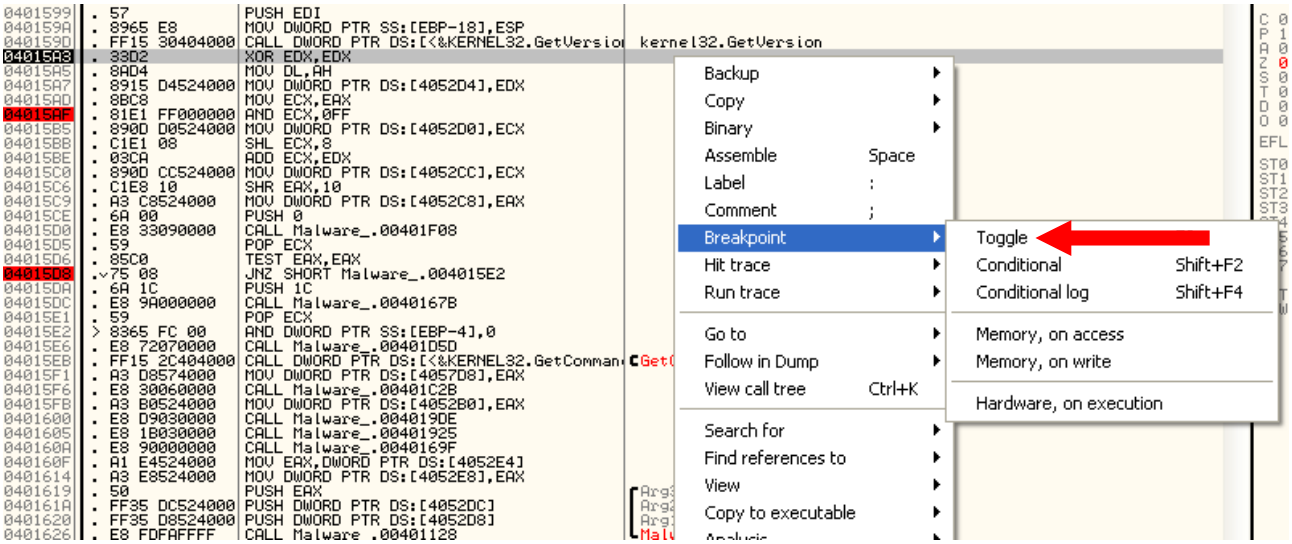
A questo punto sono andato all’indirizzo di memoria del primo quesito (0040106E):



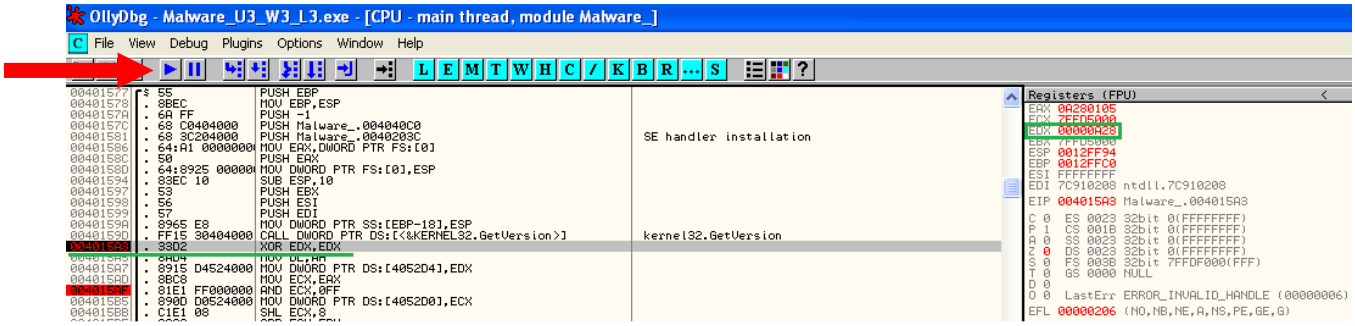
Come possiamo vedere dall’immagine qui sopra, il valore del parametro CommandLine è “cmd”.

2)

A questo punto mi sono spostato sul successivo indirizzo di memoria indicato dalla traccia (004015A3) e sono andato ad inserire un breakpoint:



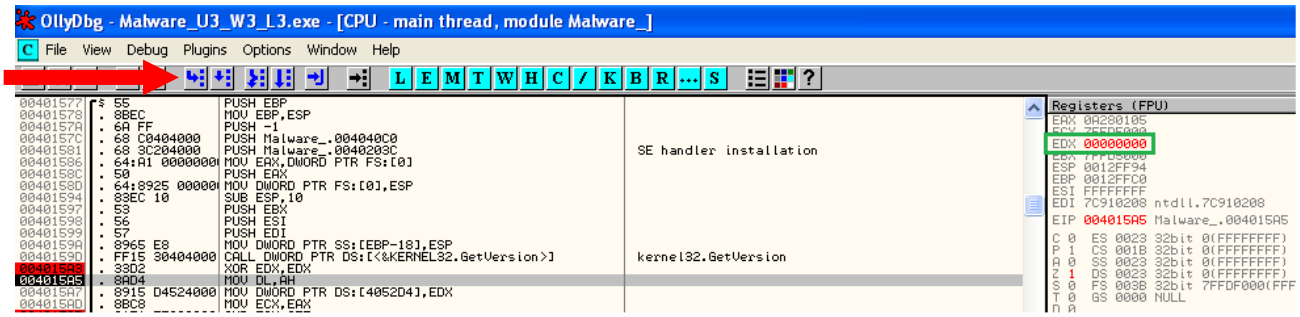
A questo punto sono andato a controllare, premendo il tasto play, il valore del registro EDX:



e ho visto che il registro ha inizialmente valore esadecimale A28, corrispondente in sistema decimale a 2600.

3)

Successivamente sono andato a eseguire uno step-into con l'apposito comando, indicato nell'immagine qui sotto dalla freccia rossa, per vedere come varia il registro EDX:



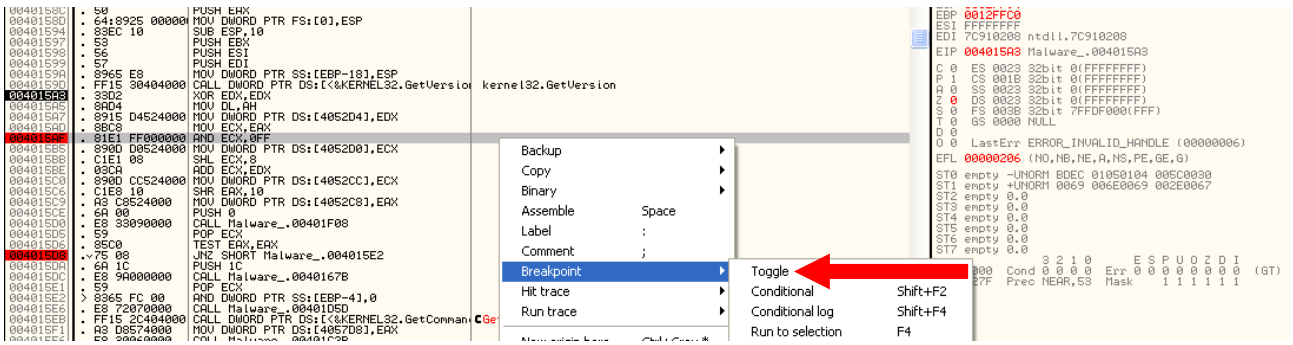
Possiamo vedere qunidi come il valore del registro che stiamo controllando assume valore 0.

4-5)

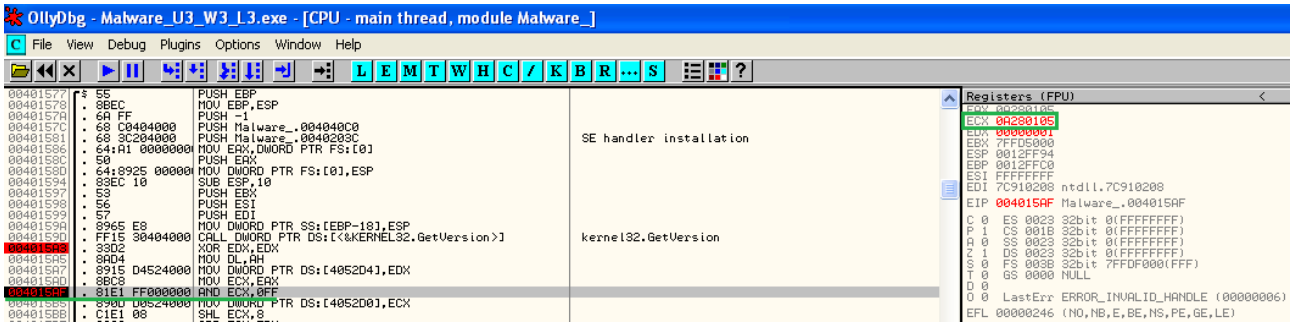
Il valore del registro EDX diventa 0 in quanto viene eseguita l'istruzione XOR (OR esclusivo). Esso è un operatore logico che restituisce in uscita 1 se e solo se gli ingressi sono diversi tra di loro. Se gli ingressi sono uguali (0-0 oppure 1-1) restituisce 0. Nel nostro caso siccome viene applicato con se stesso, qunidi 2 valori uguali, il valore restituito è 0 come si può vedere dall'immagine qui sopra.

6)

Sono quindi passato al successivo indirizzo di memoria indicato dalla traccia, 004015AF, e sono andato ad inserire un altro breakpoint come richiesto dalla traccia:



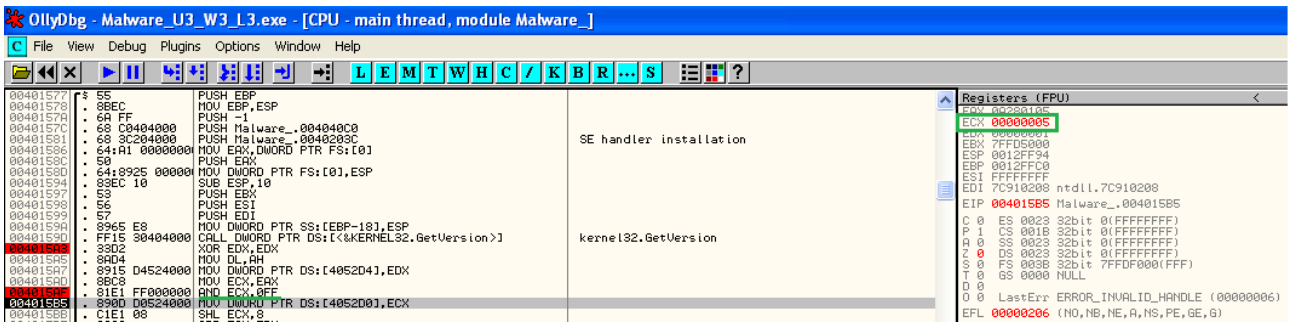
Come visto nel punto 3 sono andato a vedere il valore assunto dal registro ECX inizialmente:



Come si può vedere dall'immagine qui sopra, questo registro inizialmente ha un valore esadecimale di A280105, che in decimale equivale a 170393861.

7)

Una volta eseguito lo step-into, possiamo vedere dall'immagine qui sotto come il suo valore cambia e diventa 5:



8)

La modifica del valore inserito all'interno del registro ECX è data dall'istruzione AND. Tale operatore restituisce come valore 1 se tutti gli elementi hanno valore 1, mentre restituisce 0 in tutti gli altri casi. In questo caso viene restituito l'AND logico tra i bit di A280105 e quelli di 0FF.

9)

Dalle funzioni che vengono richiamate da questo malware penso che essi si occupi di creare una connessione remota per eseguire quindi una shell