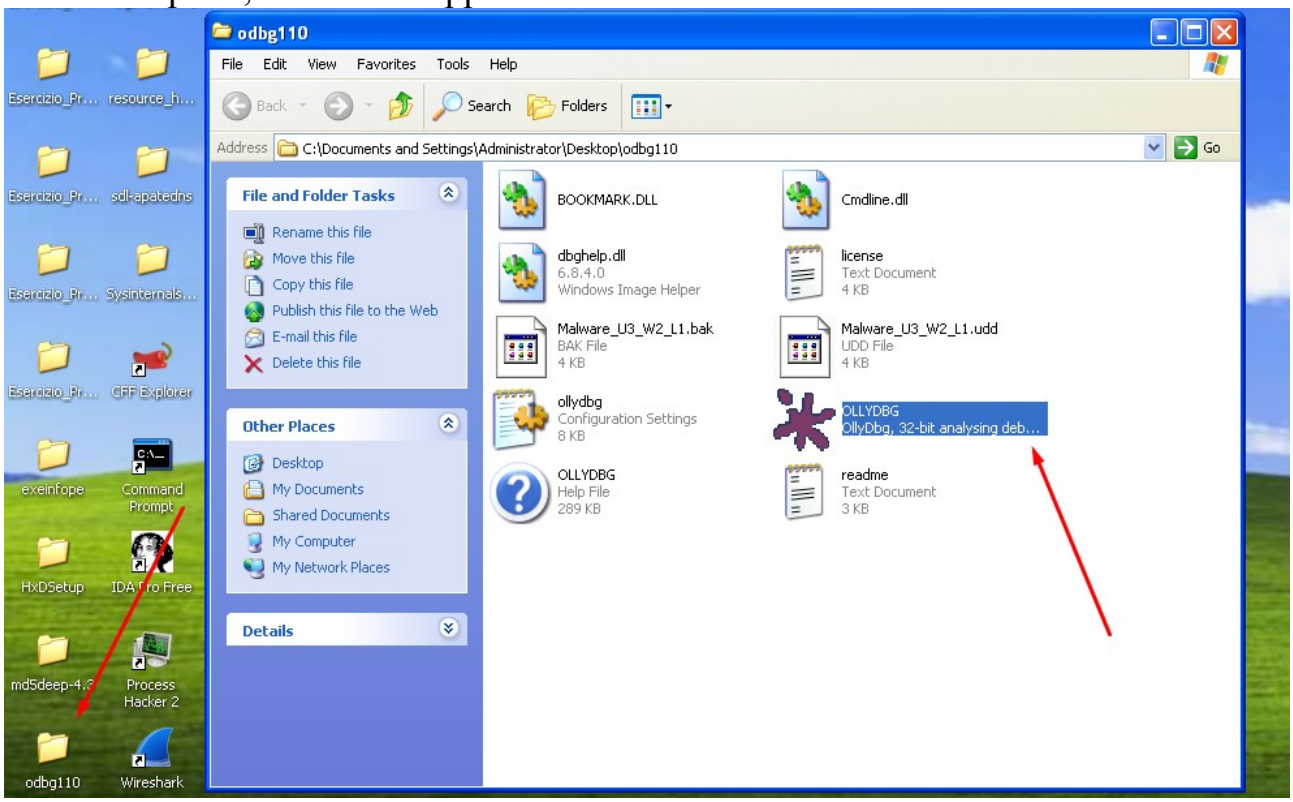
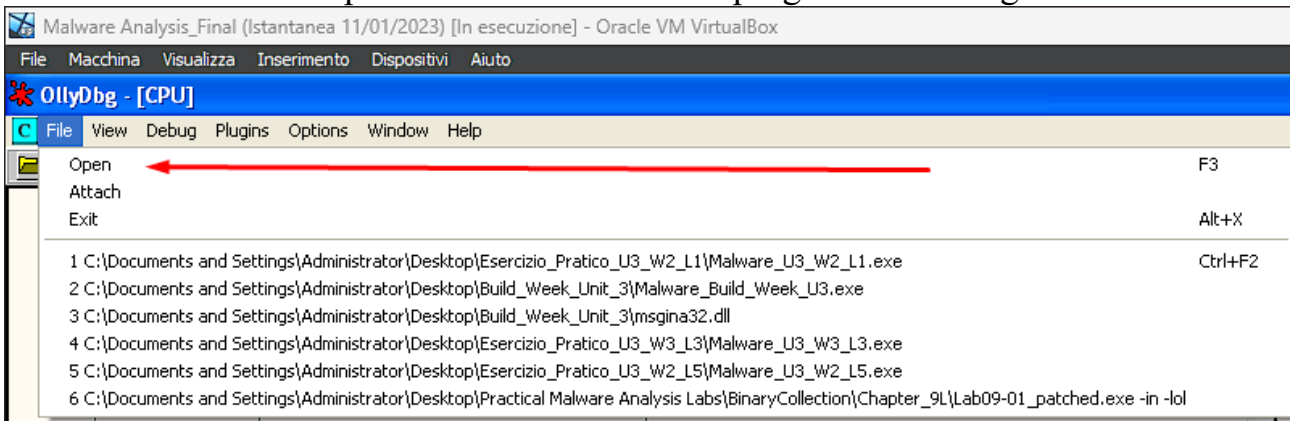
Alaimo Alessandro
18/01/2023

Report OllyDBG

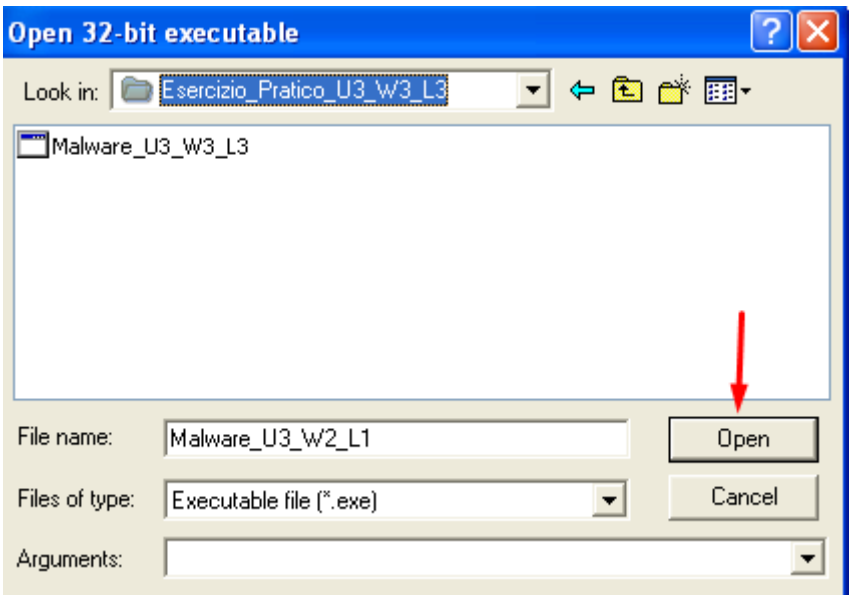
Come richiesto dall'esercizio odierno, andiamo ad aprire OllyDBG per fare debugging del file .exe richiesto. Lo ritroveremo della nostra cartella sul desktop ed una volta aperta, facciamo doppio click e diamo l'OK:



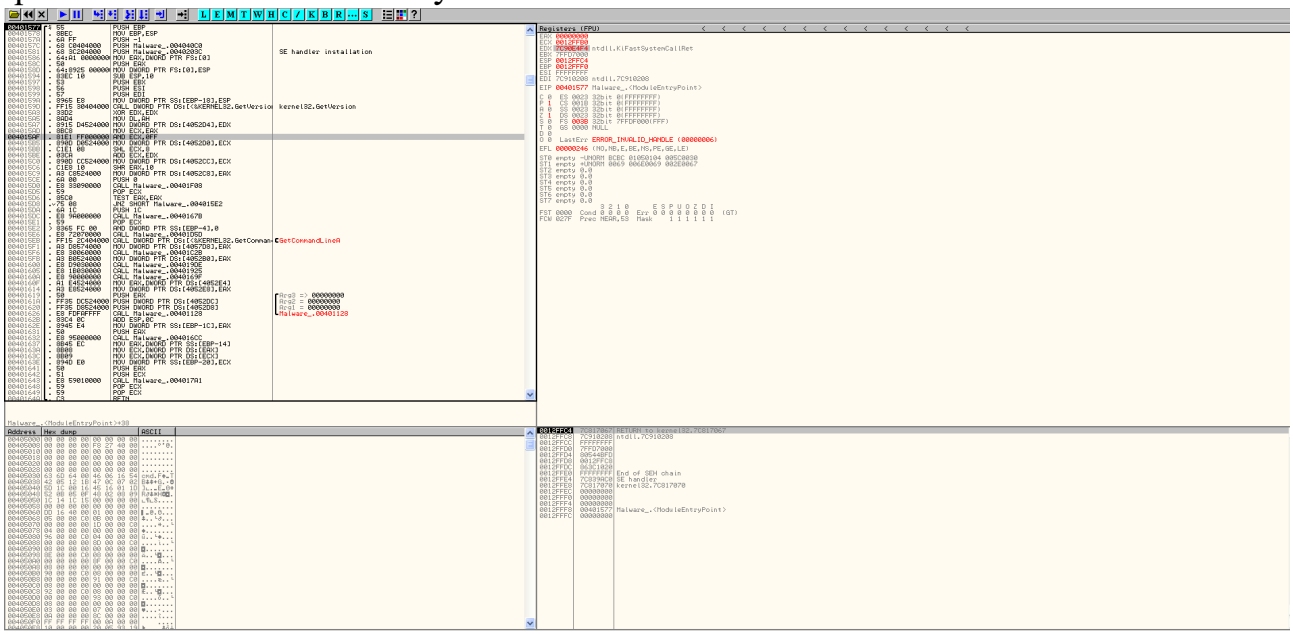
Fatto ciò andiamo ad aprire il file all'interno del programma nel seguente modo:



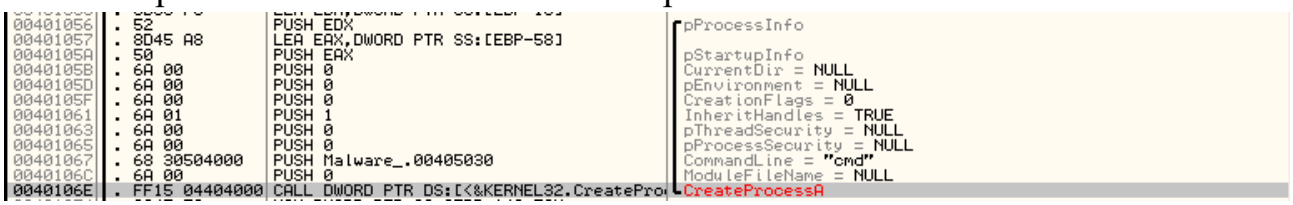
Dopodiché andiamo nella cartella del file in questione ed apriamolo:



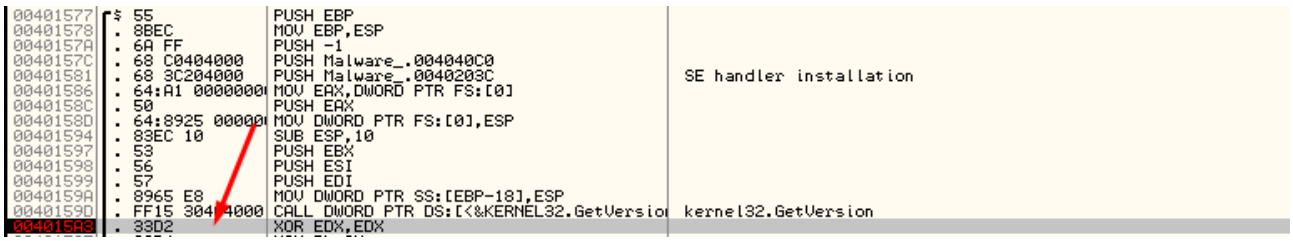
Adesso ci ritroveremo davanti diverse finestre tra cui quella più importante ovvero quella del codice in Assembly:



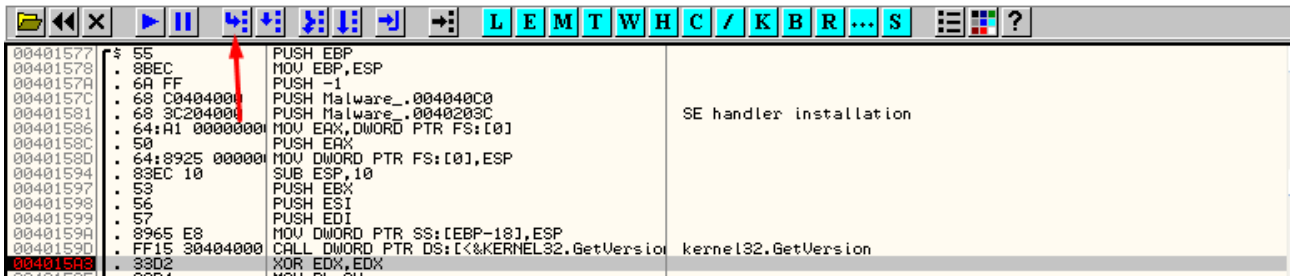
Come richiesto, saliamo fino alla stringa con indirizzo 0040106E e possiamo notare che come parametro al ***Comand Line*** viene passato ***cmd:***

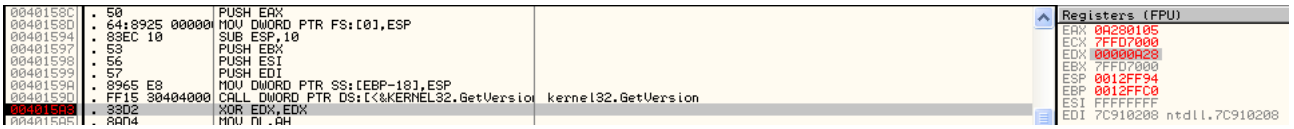


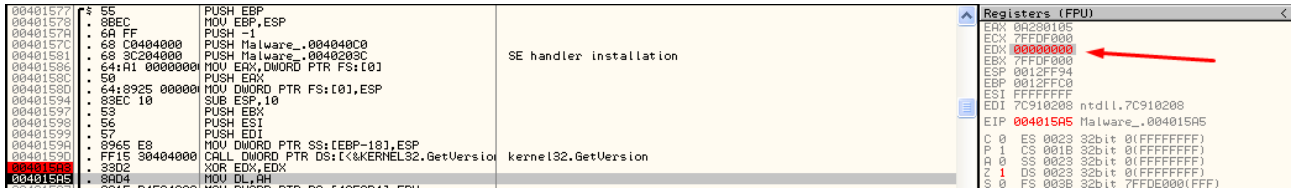
Ora andiamo a creare un breakpoint all'indirizzo 004015A3 facendo doppio click dove indicato dalla freccia ed andiamo avanti con con la freccia blu ***Run Program:***



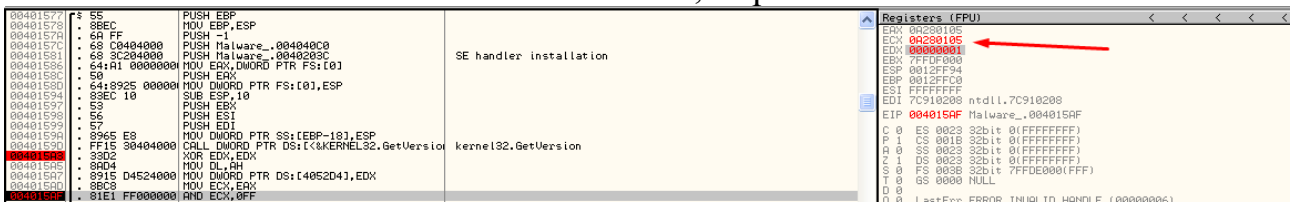
Inizialmente il valore di EDX era 2600, ma dopo l'operatore logico XOR, il risultato verrà 0 poiché l'operatore finché avrà 2 valori uguali, darà come risultato 0. Infatti possiamo vedere un prima ed un dopo del valore cliccando il pulsante ***step-in***:







Dopodiché andiamo ad inserire un secondo breakpoint all'indirizzo 004015AF ed andiamo a controllare il valore attuale di ECX, il quale è in decimale 170393861:



La stringa va ad eseguire l'operatore logico AND con il valore in decimale 170393861 (ECX) e 255 (0FF), dando come risultato 00000005:

Se si vuole fare il calcolo dell'operatore AND, si può andare alla seguente URL (https://toolslick.com/math/bitwise/and-calculator) e possiamo inserire i nostri valori e ci darà il valore come di seguito:

Calculation

Type	Decimal	Binary
Input 1	170393861	10100010100000000000100000101
Input 2	000000255	00000000000000000000011111111
Final Result	000000005	00000000000000000000000000101

Ipotizzo che la funzione di questo Malware sia quello di creare una backdoor per avere modo di eseguire codici in remoto, e lo deduco dal fatto che il Malware crea un Socket andandosi a connettere ad esso, e queste sono le stringhe di codice da cui l'ho dedotto: