

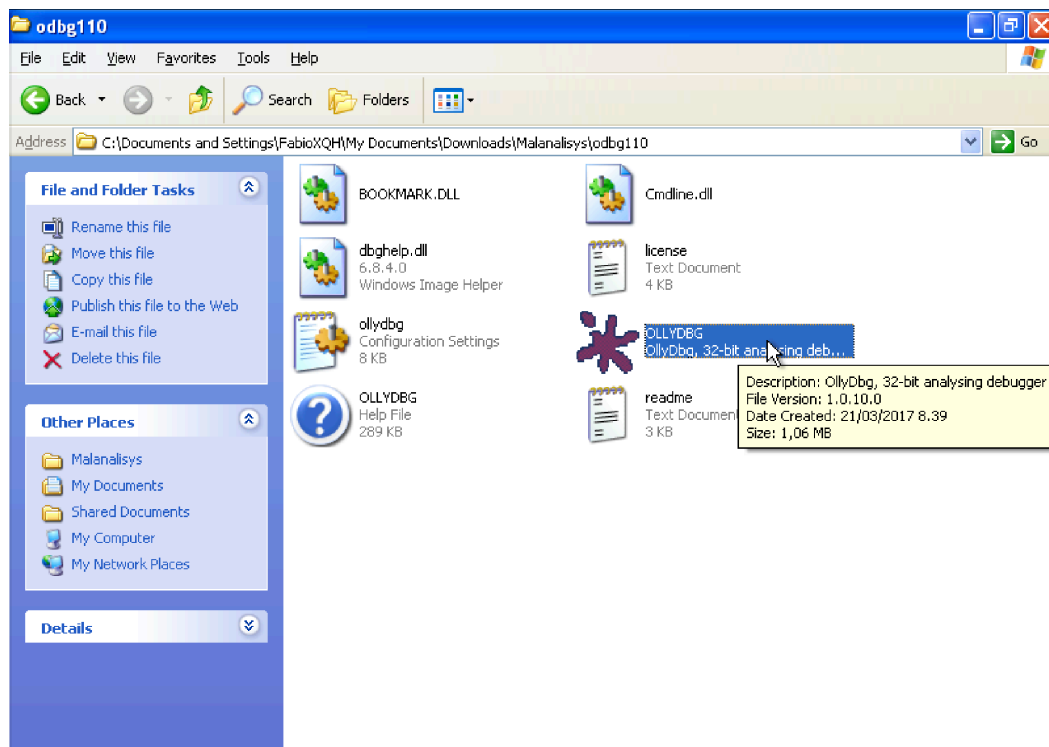
ANALISI DINAMICA AVANZATA CON OllyDGB

Traccia:

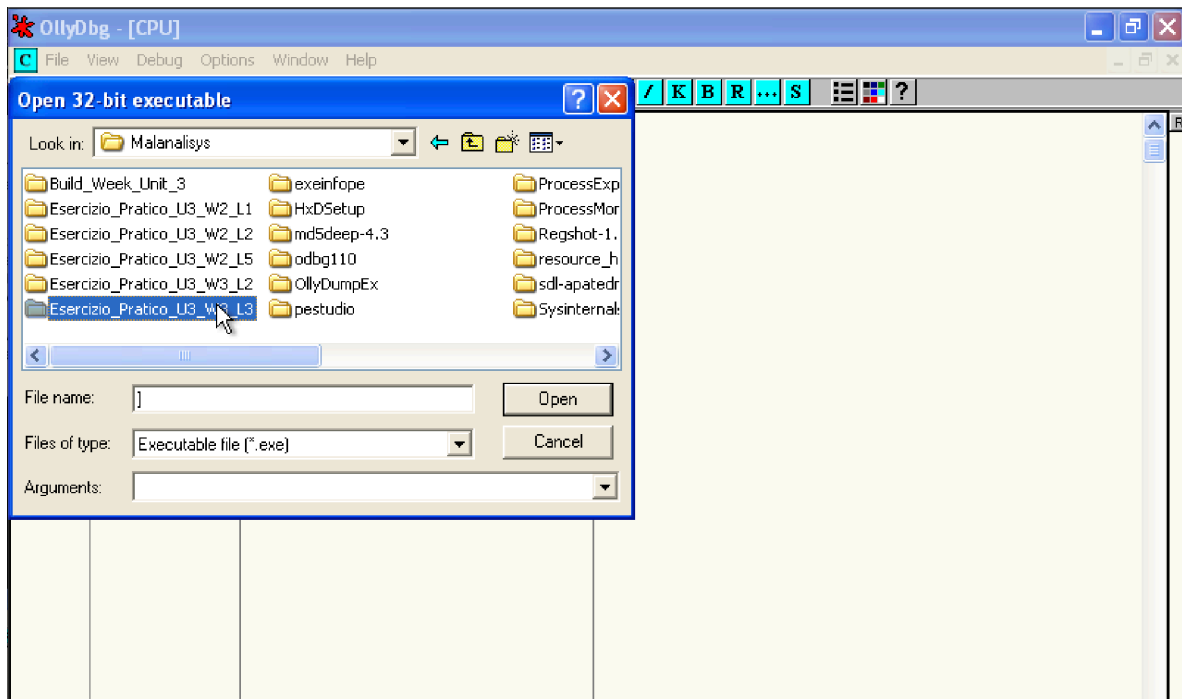
Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando **OlllyDBG**.

- 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

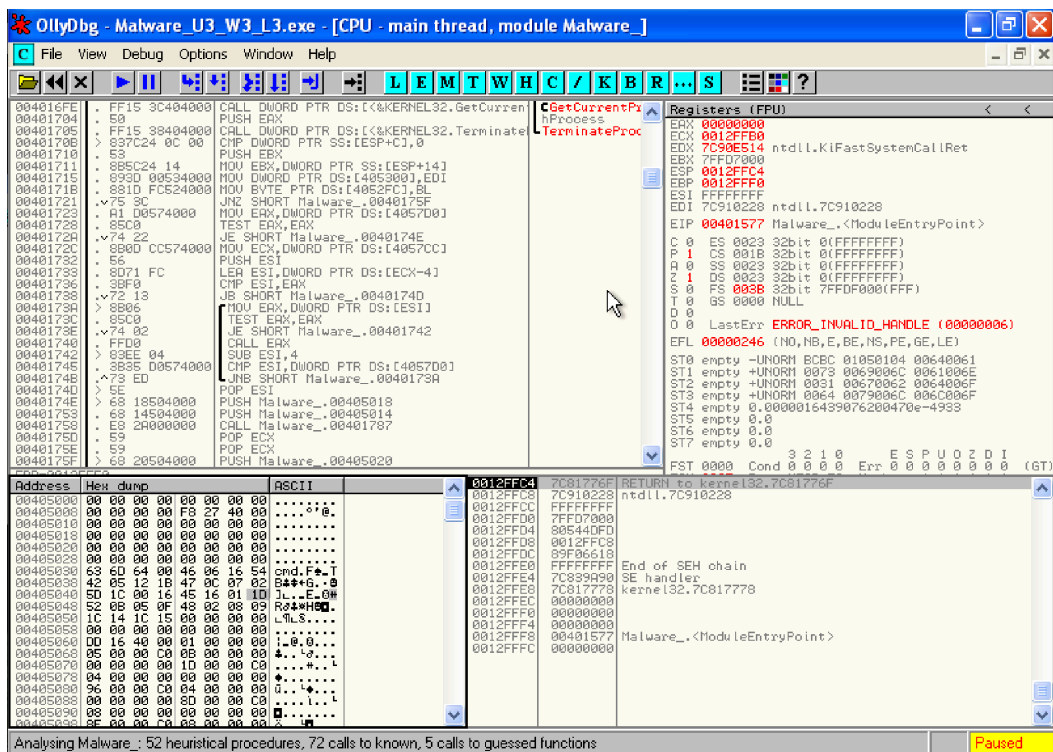
Per prima cosa andiamo ad aprire il programma “OLLYDBG” contenuto nella nostra macchina virtuale.



Una volta all'interno del programma andiamo a prelevare il file che vogliamo analizzare cliccando sull'icona Open new executable in alto a sinistra.

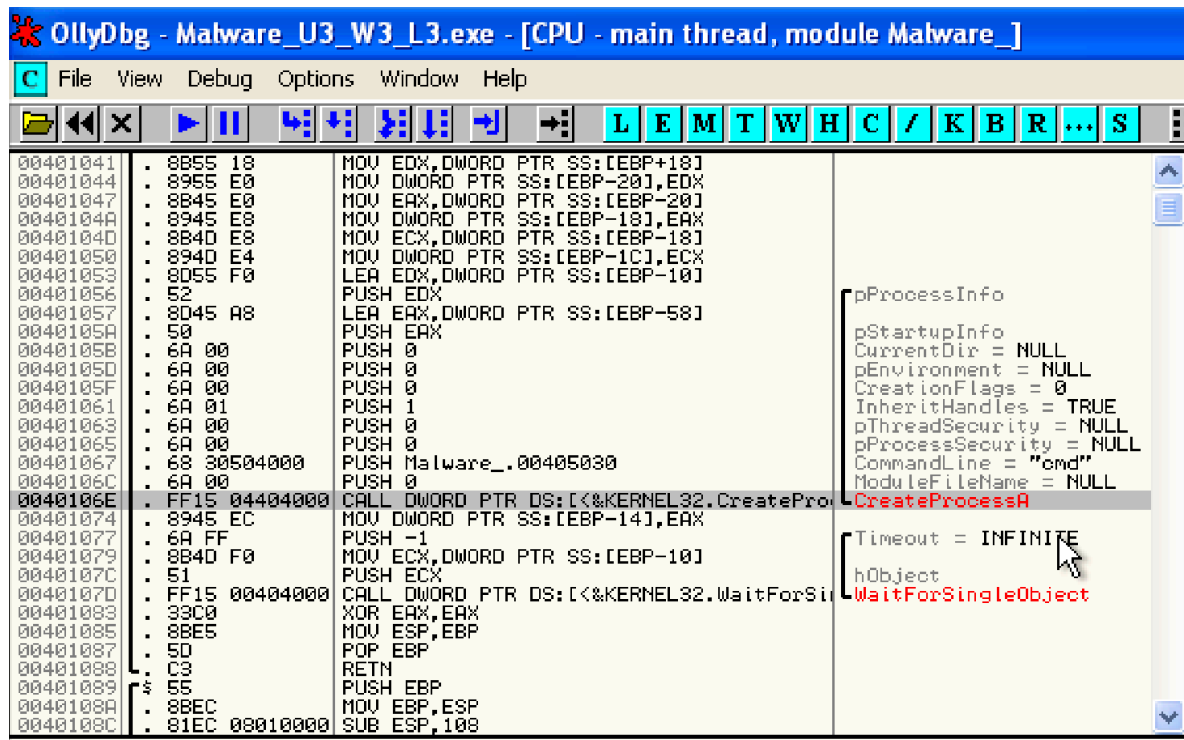


Selezionato il file ci ritroveremo questa schermata dove sono indicati i diversi indirizzi di memoria, registri e processi che il malware andrà ad eseguire.

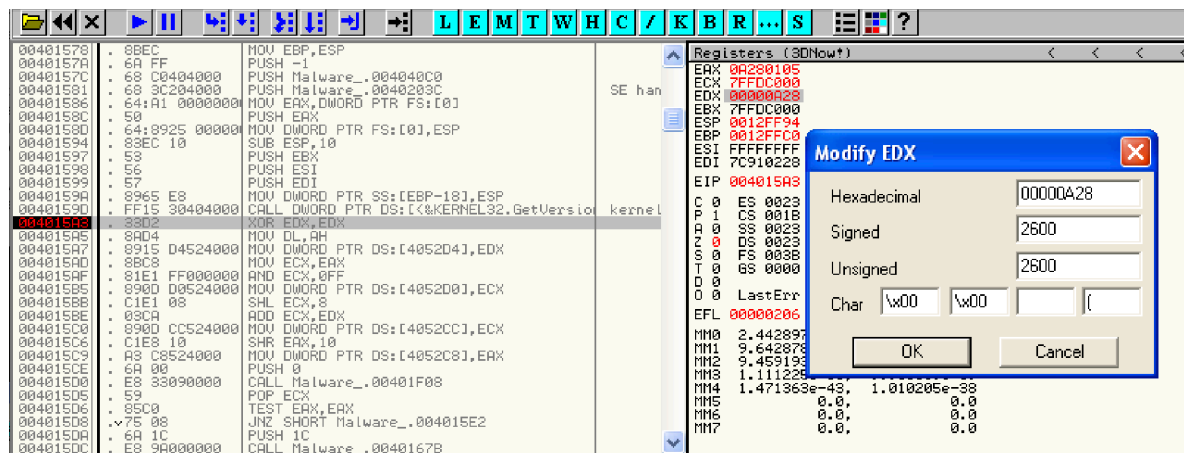


Come richiesto dall'esercizio, per prima cosa andiamo ad analizzare l'indirizzo "0040106E".

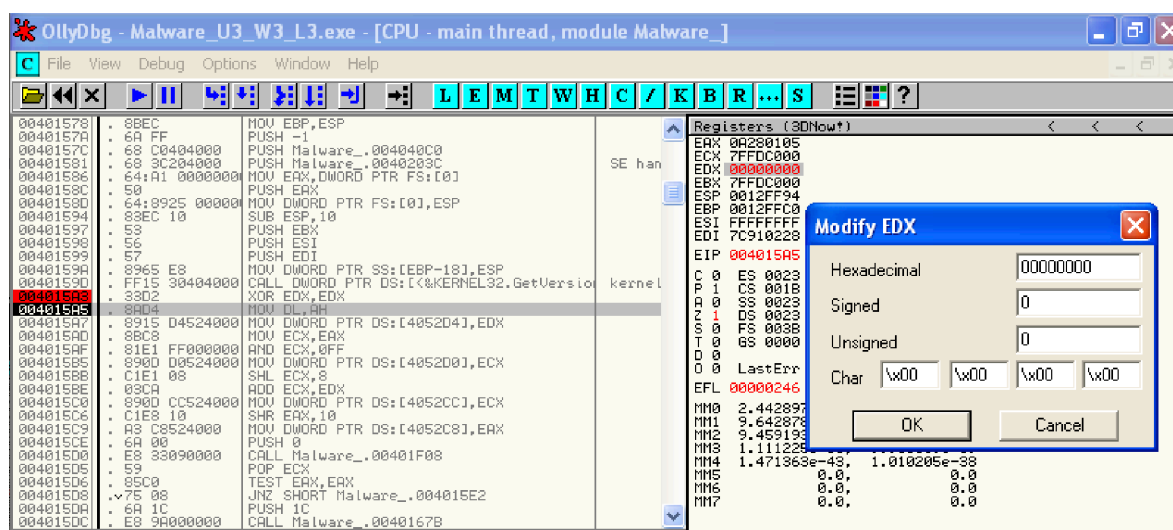
Come possiamo vedere il parametro Command line è dato come "cmd".



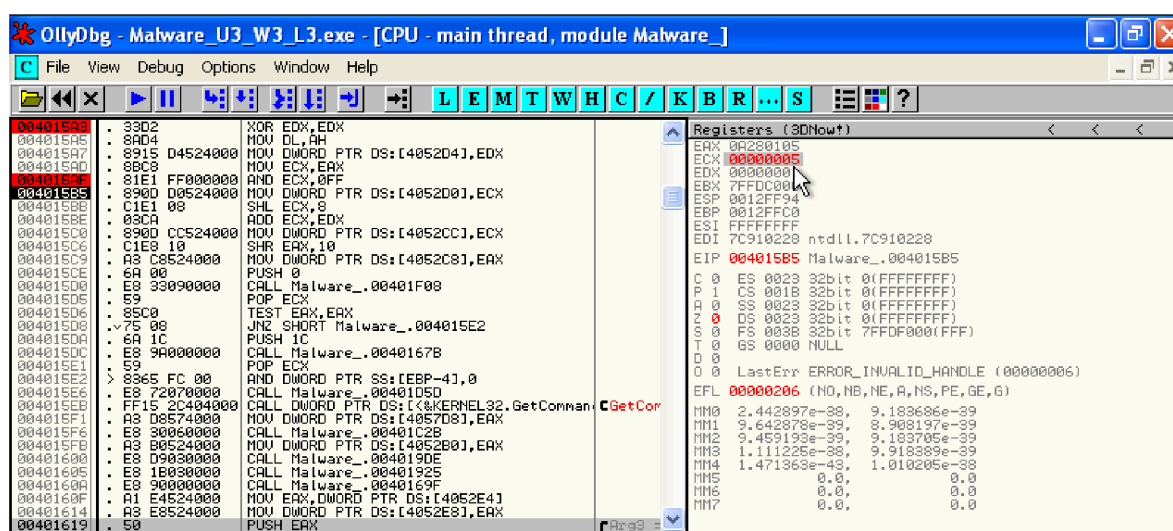
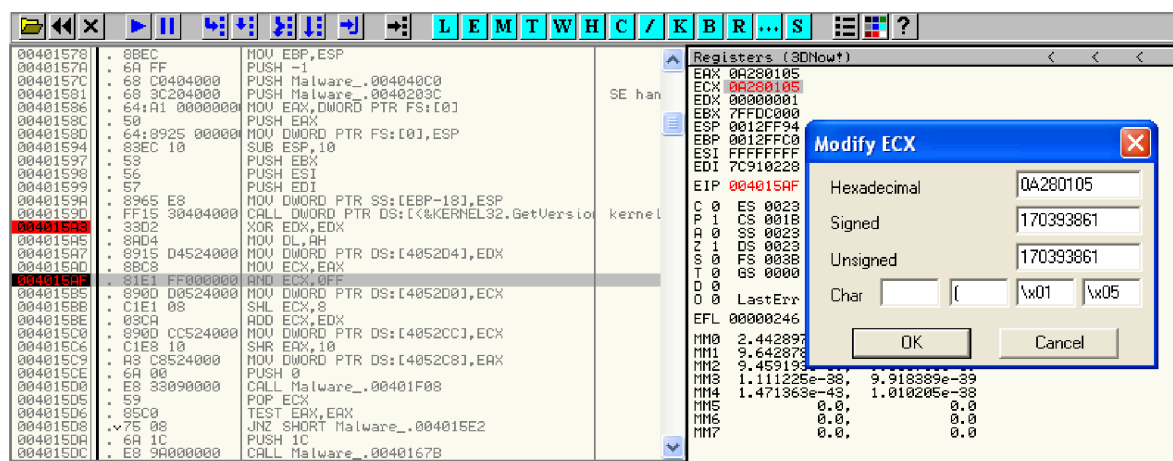
Ora andiamo come richiesto dall'esercizio andiamo a creare un breakpoint all'indirizzo 004015A3, ottenendo come risultato 2600.



Ora andiamo ad effettuare uno "step into", e possiamo notare subito come il valore di (EDX) sia cambiato da 2600 a 0. Questo è dovuto al fatto che l'operatore (XOR) finché avrà due operatori uguali darà come risultato 0.



Ora ripetiamo lo stesso procedimento però ad un indirizzo di memoria diverso ovvero il numero 004015AF.
 Come richiesto dall'esercizio, creando un breakpoint otteniamo come valore "ECX" 170393861.
 Successivamente effettuando uno "step into" possiamo vedere come "ECX" esso venga trasformato in valore decimale 00000005.



Osservando questi dati, si può presumere che questo Malware abbia la funzione di creare una backdoor per poter eseguire i codici in remoto.
 Questa teoria viene presa in considerazione in quanto il Malware crea un Socket

andandosi a connettersi ad esso, e queste sono le stringhe di codice da cui abbiamo dedotto ciò.

00401259	. 8085 68FEFFFF	LEA EAX,DWORD PTR SS:[EBP-198]	
0040125F	. 50	PUSH EAX	
00401260	. 68 02020000	PUSH 202	
00401265	. FF15 9C404000	CALL DWORD PTR DS:[&WS2_32.#115>]	pWSAData RequestedVersion = 202 (2
00401268	. 8985 4CFEFFFF	MOV DWORD PTR SS:[EBP-1B4],EAX	WSAStartup
00401271	. 83BD 4CFEFFFF	CMP DWORD PTR SS:[EBP-1B4],0	
00401278	. 74 0A	JE SHORT Malware_.00401284	
0040127A	. B8 01000000	MOV EAX,1	
0040127F	. E9 52010000	JMP Malware_.00401306	
00401284	> 6A 00	PUSH 0	Flags = 0
00401286	. 6A 00	PUSH 0	Group = 0
00401288	. 6A 00	PUSH 0	pWSAprotocol = NULL
0040128A	. 6A 06	PUSH 6	Protocol = IPPROTO_TCP
0040128C	. 6A 01	PUSH 1	Type = SOCK_STREAM
0040128E	. 6A 02	PUSH 2	Family = AF_INET
00401290	. FF15 00404000	CALL DWORD PTR DS:[&WS2_32.WSASocket@	WSASocket@
00401296	. 8985 FCFCFFFF	MOV DWORD PTR SS:[EBP-304],EAX	
0040129C	. 83BD FCFCFFFF	CMP DWORD PTR SS:[EBP-304],-1	
004012A3	. 75 0A	JNZ SHORT Malware_.004012AF	
004012A5	. B8 01000000	MOV EAX,1	
004012AA	. E9 27010000	JMP Malware_.00401306	
004012AF	> 808D 10FEFFFF	LEA ECX,DWORD PTR SS:[EBP-1F0]	
004012B5	. 51	PUSH ECX	Arg2
004012B6	. 8095 50FEFFFF	LEA EDX,DWORD PTR SS:[EBP-1B0]	Arg1
004012BC	. 52	PUSH EDX	Malware_.00401089
004012BD	. E8 C7FDFFFF	CALL Malware_.00401089	
004012C2	. 83C4 08	ADD ESP,8	
004012C5	. 8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
004012C8	. 8B45 F8	MOV EAX,DWORD PTR SS:[EBP-8]	
004012CB	. 50	PUSH EAX	
004012CC	. FF15 A4404000	CALL DWORD PTR DS:[&WS2_32.#52>]	Name gethostbyname