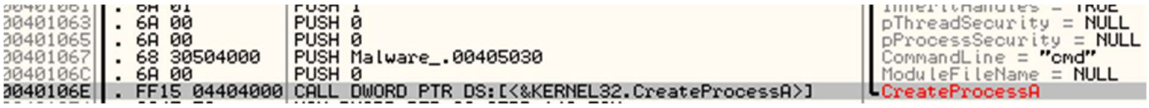
ESERCIZIO S11-L3

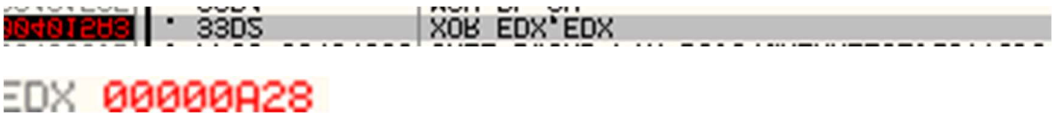
Lo scopo dell'esercizio di oggi è quello di usare "OllyDbg" usando il Malware_U3_W3_L3 e rispondere ai seguenti quesiti:

- 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?
- 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. Che istruzione è stata eseguita?
- Inserite un secondo "breakpoint" all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite uno "step-into". Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
- Spiegare a grandi linee il funzionamento del malware.

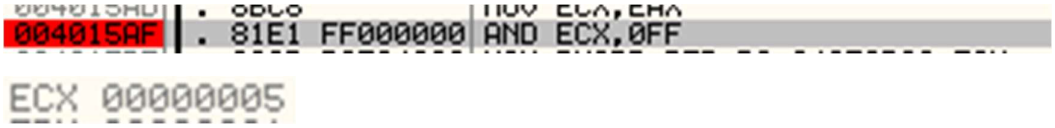
1. Il valore del parametro "commandline" che viene passato sullo stack è "cmd".



2. Eseguendo uno step-into il valore del registro EDX è 0 perché XOR restituisce 0 se i due operandi sono uguali.



3. Stesso procedimento per l'indirizzo di memoria "004015AF". Il valore di "ECX" dopo lo "step-into" è 5. In questo caso avviene un'operazione "AND" e il risultato sono le ultime due cifre.



4. Per capire a grandi linee di che tipo di malware si tratti, ho ricavato l'hash e l'ho caricato su "VirusTotal". Il tool ha dato come risposta che si tratti in generale di un trojan ma non ne specifica il tipo. Quindi potrebbe trattarsi di una backdoor, downloader, spyware e così via.