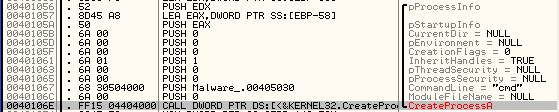
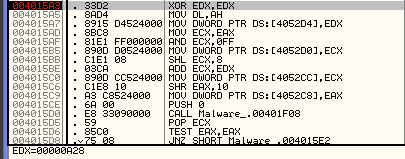
Pratica di OllyDBG

* 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, motivando la risposta e 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.
* BONUS: spiegare a grandi linee il funzionamento del malware

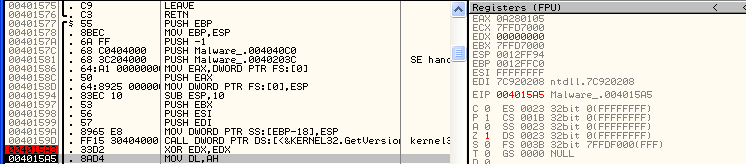
Nella funzione “CreateProcessA”, a questo determinato indirizzo 0040106E, il parametro “CommandLine” ha come valore “cmd”. Ciò significa che si sta richiedendo l'esecuzione del prompt dei comandi di Windows.



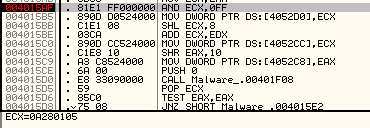
Il valore del registro EDX all’indirizzo 004015A3 prima di effettuare questa operazione “XOR EDX, EDX” è di 00000A28



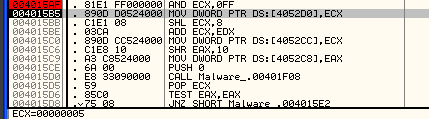
Questa istruzione XOR restituisce 1 per ogni coppia di bit diversi e 0 per ogni coppia di bit uguali, per questo essendo che l’operazione viene effettuata tra EDX e sé stesso il risultato sarà 0. Azzerando così il valore di EDX.



Il valore del registro ECX all’indirizzo 004015AF prima di effettuare l’operazione “AND ECX, 0FF” è di 0A280105



“AND ECX, 0FF”: L’operazione AND tra due operandi (A e B) restituirà 1 solo se entrambi A e B sono 1; in tutti gli altri casi, restituirà 0. ECX=00000005



Da una macro-analisi del malware su OllyDBG si può notare alcune funzioni e chiamate di librerie che fanno presumere che il malware cerchi di connettersi alla rete internet, di conseguenza possiamo presumere che il malware sia una backdoor.

