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 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?

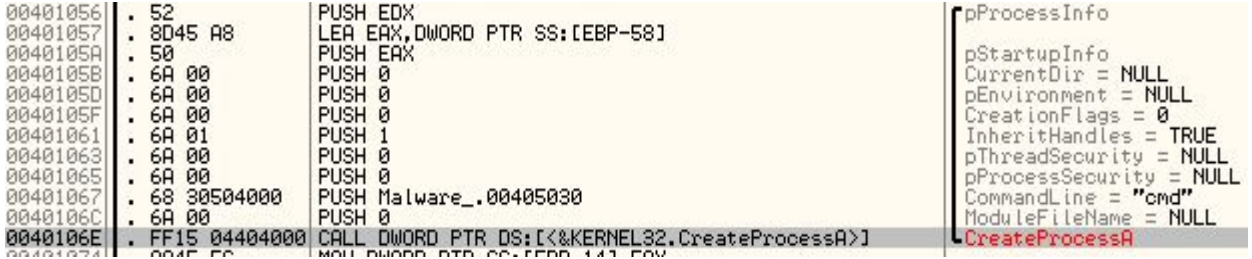
Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta.

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

Qual è il valore del parametro «CommandLine» che viene passato sullo stack?



Come vediamo da OllyDBG il valore del parametro **CommandLine** che viene passato sullo stack a seguito della chiamata alla funzione è **cmd**.

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.

Una volta impostato il **breakpoint** all' indirizzo di memoria **004015A3** posso andare a verificare il valore del registro **EDX** nella tabella dei registri. Come si vede dallo screenshot, questo valore è **00000A28**.

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta.

Una volta eseguito lo **step-into**, vediamo come il valore del registro **EDX** sia cambiato in **00000000**.

Attraverso lo step-into viene eseguita l' istruzione **XOR** che è equivalente ad inizializzare a **0** una variabile. L' istruzione che viene eseguita, nello specifico, è **XOR EDX, EDX**.

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

Dopo aver impostato un nuovo breakpoint sull' indirizzo **004015AF**, vediamo come il valore del registro **ECX** sia **0A280105.**

Eseguite uno step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Dopo aver eseguito lo step-into, il valore del registro **ECX** cambia in **00000005**

Questo è il risultato dell' esecuzione dell' istruzione **AND** sui bit nel registro **ECX** ed il valore esadecimale **000000FF.**

BONUS: spiegare a grandi linee il funzionamento del malware

Dopo aver ricavato l’ hash del file eseguibile tramite il tool **md5deep** ed averlo analizzato con Virus Total, è venuto fuori che il malware sembrerebbe essere un **Trojan**.