**OllyDBG**

**TRACCIA**

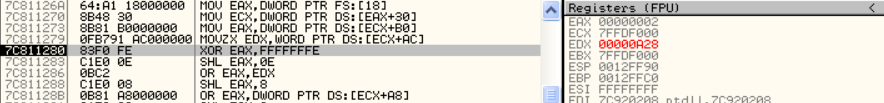
Fate riferimento al malware: Malware\_U3\_W3\_L3, presente all’interno della cartella Esercizio\_Pratico\_U3\_W3\_L3sul desktop della macchina virtuale dedicata all’analisi dei malware.   
Rispondete ai seguenti quesiti utilizzando OllyDBG.   
1) All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?   
2) Inserite un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX?   
3-4) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX, motivando la risposta.   
5) Che istruzione è stata eseguita?   
6-7) Inserite un secondo breakpoint all’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX?  
8) Che istruzione è stata eseguita?  
BONUS: Spiegare a grandi linee il funzionamento del malware.  
 **ESERCIZIO**

1) Aprendo il malware su OllyDBG, possiamo notare come all’indirizzo 0040106E venga effettuata una chiamata alla funzione CreateProcessA, prendendo come parametro CommandLine, con valore “cmd”.

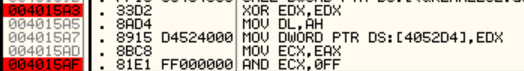


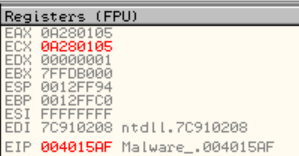
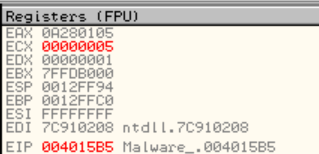
2) Dopo aver inserito un breakpoint all’indirizzo 004015A3, andiamo a controllare il valore di EDX.   
Prima di eseguire il programma, possiamo notare che il contenuto di EDX = 7C90E4F4.

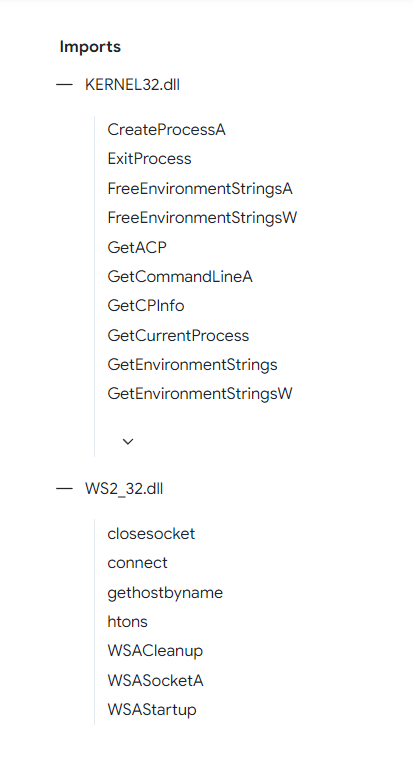


3-4) Dopo aver eseguito uno step-into nella funzione “Kernel32.GetVersion”, il valore nel registro EDX = 00000A28 (riquadro rosso).

5) Questo cambio di valore è dovuto all’istruzione “MOVZX” (riquadro verde), in cui il valore di ECX+AC viene copiato in EDX.  
MOVZX sposta un dato da un registro o una locazione di memoria da 8 o 16 bit in un registro o locazione di memoria di dimensioni più grandi, da 16 o 32 bit.  
  
  
6-7) Dopo aver inserito un secondo breakpoint all’indirizzo 004015AF (riquadro rosso), andiamo a controllare il valore di ECX (riquadro verde).   
Il contenuto di ECX = 0A280105.   
Dopo aver eseguito il programma,  
il valore di ECX = 00000005 (riquadro arancione).





8) Questo cambio di valore è dovuto alle istruzioni (riquadro blu):  
a. “MOV ECX, EAX” che copia il contenuto di EAX dentro ECX.  
b. “AND ECX, 0FF” in cui il valore di ECX+AC viene copiato in EDX.  
  
  
  
  
  
BONUS) Tramite CFF Explorer ci procuriamo l’hash del malware e lo andiamo ad analizzare su VirusTotal.   
Possiamo notare che è classificato come “Trojan”  
e, controllando gli imports utilizzati, utilizzi la libreria  
“WS2\_32.dll” che contiene le API usate dalla maggior  
parte delle applicazioni della rete e di Internet.  
