Pratica S11/L3 - Malware analysis con OllyDBG

L'esercizio di oggi consiste nell'utilizzare OllyDBG per effettuare un analisi dinamica avanzata di un malware presente sulla nostra macchina e rispondere a questi quesiti:

1.All'indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

2.Inserite un breakpointsoftware 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)

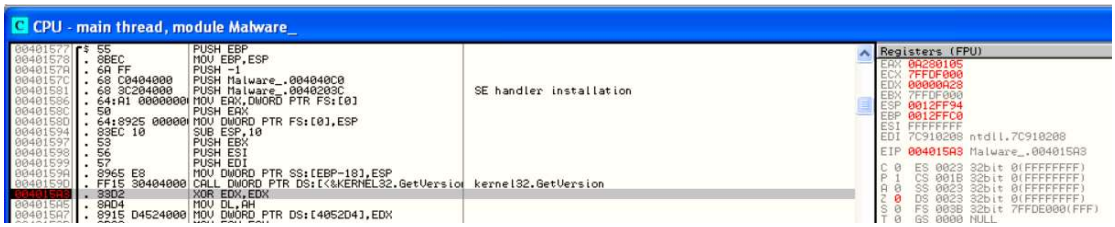
3.Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7)Spiegate quale istruzione è stata eseguita (8).

BONUS: spiegare a grandi linee il funzionamento del malware

1.All'indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

Il parametro <commandLine> che viene passato sullo stack è "cmd"

2.Inserite un breakpointsoftware 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)



Il valore del registro EDX all'indirizzo 004015A3 è di 00000A28.

Eseguo uno <step-into>.

Possiamo vedere che il valore di EDX è diventato 00000000 poichè viene fatto uno XOR tra EDX ed EDX quindi si effettua uno 'zeroing' per settare a 0 il valore di EDX, perchè il risultato di uno XOR tra due valori uguale risulta sempre 0.

3.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).

Il valore di ECX all'indirizzo 004015AF è 0A280105.

Eseguo uno <step-into>.

Il valore di ECX diventa 00000005 perchè viene fatta l'istruzione AND tra ECX e 0FF, per arrivare a questo risultato possiamo trasformare i due valori in binario e eseguire l'AND tra i due.

BONUS: spiegare a grandi linee il funzionamento del malware

Sfruttando il tool CFF Explorer ho ricavato l'hash del malware e controllando su virus total risulta essere un trojan.