Compito S11-L3

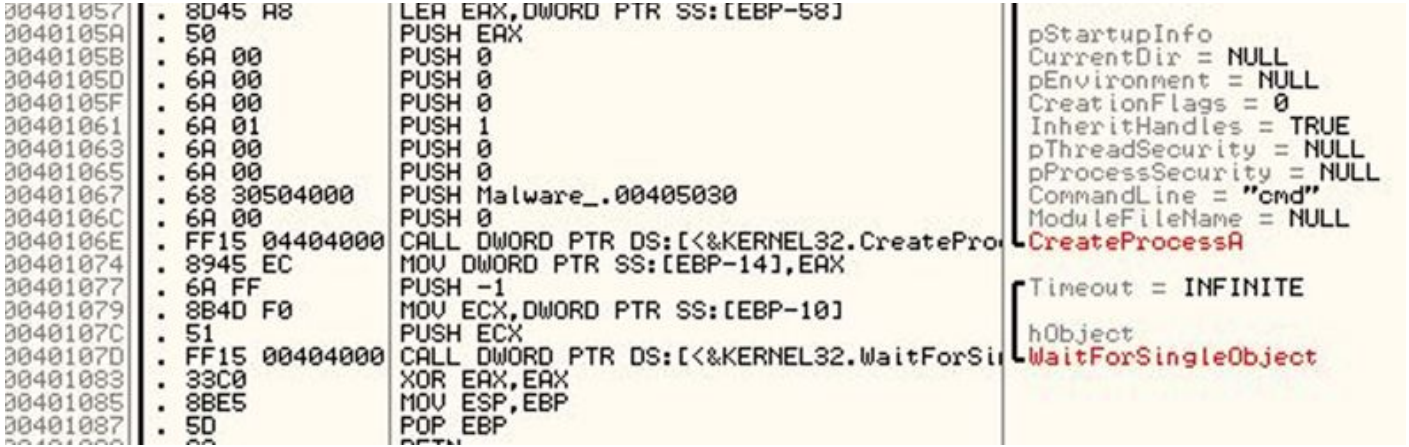
Traccia

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.

- 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? (1)
- Inserite un breakpoint software 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)
- 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

Il valore del parametro è “CMD” ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo 00401067.



2, 3, 4, 5

Una volta configurato il breakpoint, clicchiamo su “play”, il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è “00000A28”. Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà 0.

Prima

Dopo

6,7

Configuriamo il secondo breakpoint. Il valore del registro ECX è “0A280105”.

Dopo lo step-into il valore del registro ECX è stato modificato in “00000005” in quanto è stata eseguita l’istruzione AND ECX, FF.

8

Nel dettaglio, l'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa portiamo entrambi i valori in formato binario e poi eseguiamo l'AND logico tra i bit.

Esadecimale	Binario
0A280105	0000 1010 0010 1000 0000 0001 0000 0101
FF	0000 0000 0000 0000 0000 0000 1111 1111

Il risultato è 0000 0000 0000 0000 0000 0000 0000 0101
Che in esadecimale è 5. (oppure 00000005)