OllyDBG

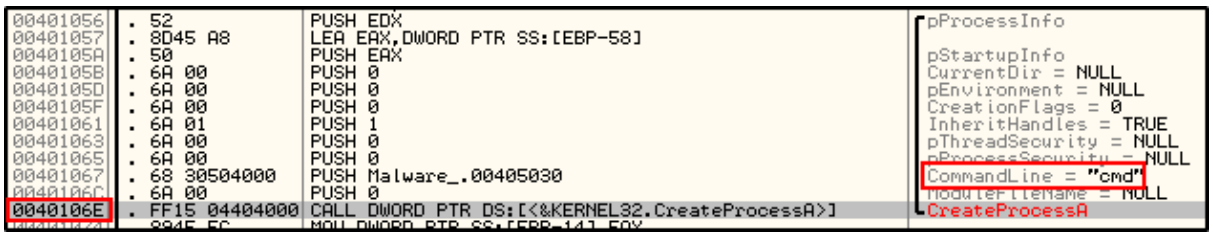
Traccia

Facendo riferimento al malware: Malware_U3_W3_L3 rispondere 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. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX
4. Motivate la risposta.
5. Che istruzione è stata eseguita?
6. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
7. Eseguite un step-into. Qual è ora il valore di ECX?
8. Spiegate quale istruzione è stata eseguita.
9. BONUS: spiegare a grandi linee il funzionamento del malware.

Traccia 1

Il valore passato è "cmd" ovvero il commando prompt di Windows.



Traccia 2

Inseriamo il breakpoint nell'indirizzo richiesto e premiamo play, quindi vediamo che il valore di EDX è 00001DB1.

Traccia 3

Cliccando su Step Into il programma entra nella funzione e il valore di EDX cambia in 00000000.

Traccia 4

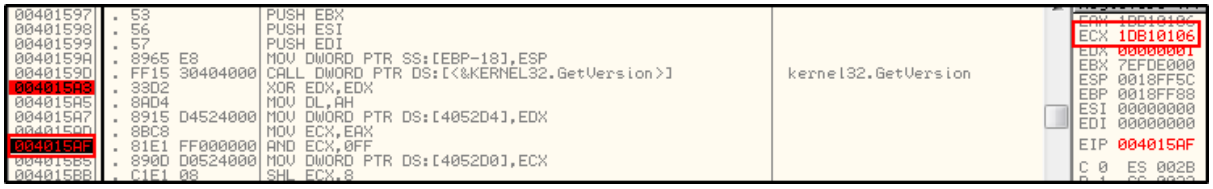
Ciò avviene perchè nell'operazione XOR (exclusive OR), l'output è 1 se i bit corrispondenti degli operandi sono diversi, e 0 se sono uguali. In questo caso viene fatto XOR paragonando EDX a se stesso quindi il risultato è 0 per ciascun bit.

Traccia 5

XOR EDX,EDX

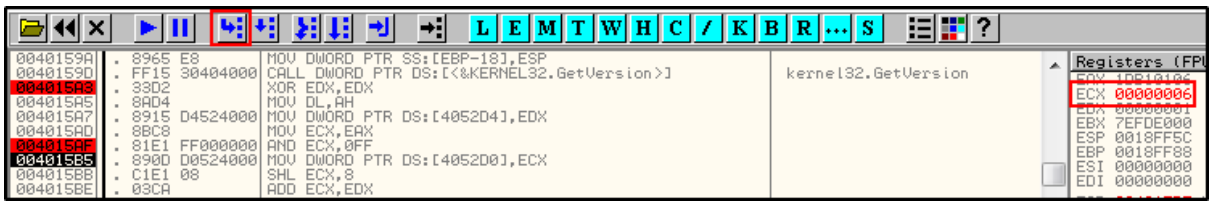
Traccia 6

Inserendo il breakpoint e premendo su play il valore di ECX diventa 1DB10106



Traccia 7

Eseguendo uno step into il valore di ECX diventa 00000006.



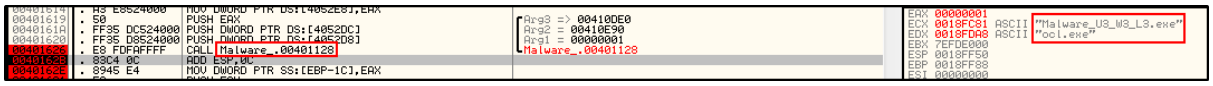
Traccia 8

E' stata eseguita AND ECX, 0FF dove avviene un AND fra i bit di ECX e 0FF dove viene restituito 1 solo se entrambi i bit sono uguali a 1.

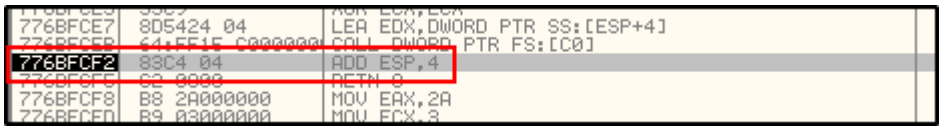
0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	=	1DB10106
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	=	0FF
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	=	00000006

Traccia 9

Usando diversi breakpoint ci accorgiamo che la funzione Malware_.00401128 dopo essere eseguita aggiunge come valori il nome del file e ocl.exe rispettivamente a ECX e EDX.



Proseguendo senza interruzioni i due valori scompaiono e il programma ferma la sua esecuzione al seguente indirizzo.



Questo fa pensare che qualcosa impedisce la corretta esecuzione del malware.