Manuel Di Gangi

S11_L3

OllyDBG

03 aprile 2024

INDICE

Traccia

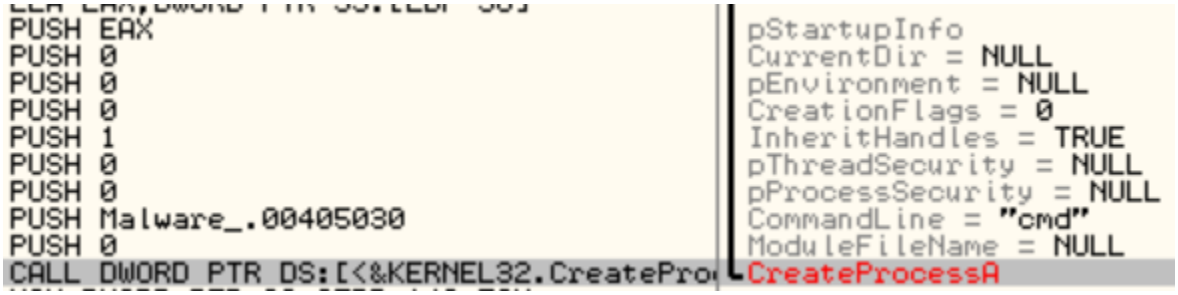
Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

1. All'indirizzo 0040106E il Malware Effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «Command Line» che viene passato sullo stack?
2. Inserite un breakpoint software all'indirizzo 004015A3.
    a. Qual è il valore del registro EDX?
    b. Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta
    c. Che istruzione è stata eseguita?
3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF.
    a. Qual è il valore del registro ECX?
    b. Eseguite un step-into. Qual è ora il valore di ECX?
    c. Spiegate quale istruzione è stata eseguita

4. BONUS: spiegare a grandi linee il funzionamento del malware

1. Parametro «Command Line»

All'indirizzo 0040106E il Malware Effettua una chiamata di funzione alla funzione «CreateProcess».



Il valore del parametro «Command Line» che viene passato sullo stack

2. Registro EDX

Inserite un breakpoint software all'indirizzo 004015A3.

2.a

Qual è il valore del registro EDX?

2.b

Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?

2.c

L'istruzione eseguita è lo XOR logico del registro EDX, tale operazione ritorna 1 se e solo se i due valori sono diversi tra loro, ma EDX è sempre uguale EDX perciò tale operazione resetterà il registro a 0.

3. Registro ECX

Inserite un secondo breakpoint all'indirizzo di memoria 004015AF.

3.a

Qual è il valore del registro ECX?

3.b

Eseguite un step-into. Qual è ora il valore di ECX?

3.c

All’indirizzo indicato dalla traccia viene effettuato un AND logico tra il contenuto del registro ECX ed il numero esadecimale FF. Come illustrato di seguito il nuovo contenuto del registro è il risultato dell’operazione.

Operazione	Hex	Bin
AND	1DB1 0106	0001 1101 1011 0001 0000 0001 0000 0110
	FF	1111 1111
	0000 0006	0000 0000 0000 0000 0000 0000 0000 0110

4. Funzionamento del malware