S11 L3

Analisi Dinamica Avanzata

Daniele Zizzi

Traccia:

Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

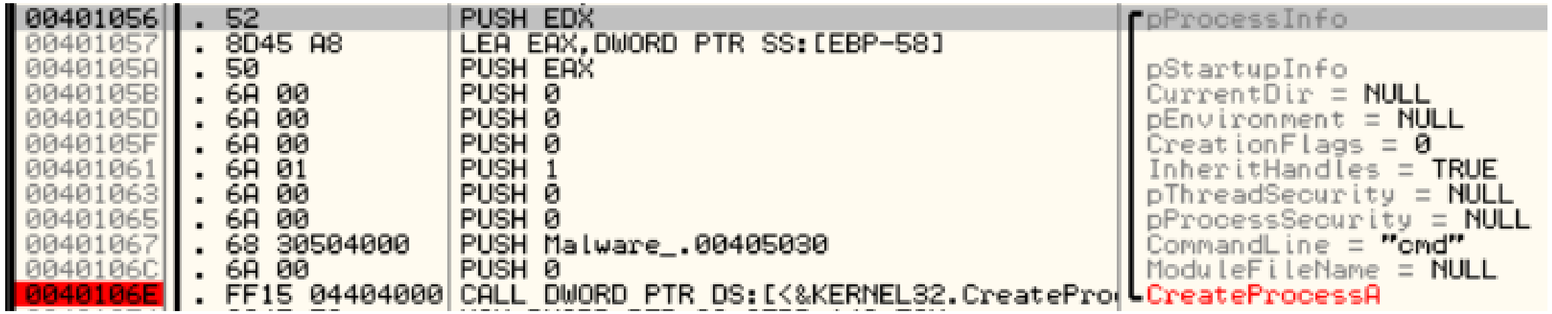
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo **stack**? **(1)**

- 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

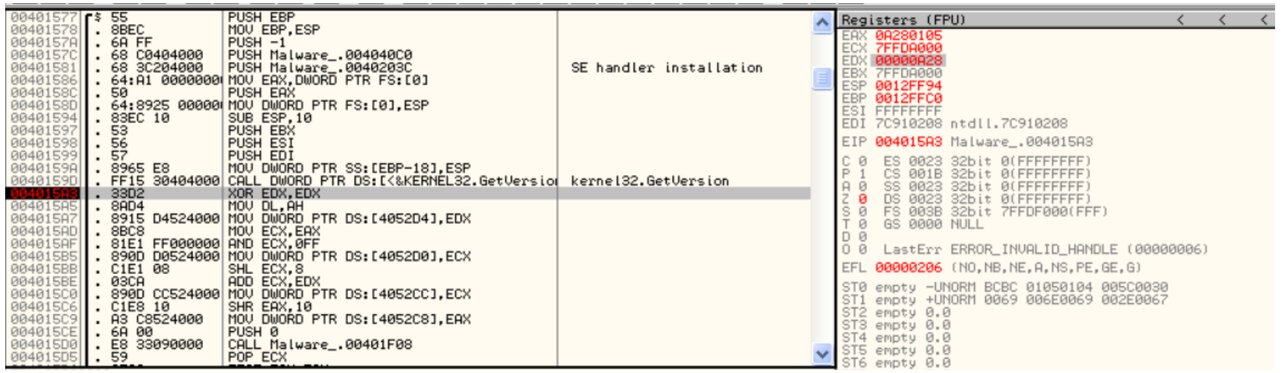
Effettua una chiamata alla dll Kernel32 e crea un processo. Come parametro in CommandLine, gli passa “cmd”.
Ipotizzo che, le seguenti righe di codice, aprono un prompt dei comandi.

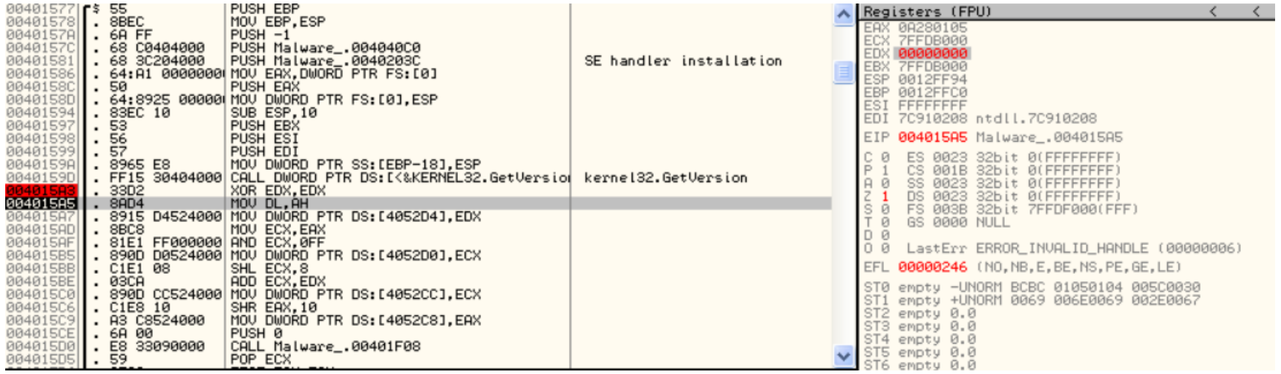


Il valore del registro di EDX è A28.

Dopo l’operazione logica XOR tra EDX ed EDX, quindi se stesso, il risultato è 0. Poichè XOR(exclusive OR), viene usato per pulire/impostare a 0 un registro.

La XOR da come risultato 1(vero), solo se gli ingressi sono diversi tra di loro. Se entrambi gli ingressi hanno lo stesso valore, l'uscita sarà 0 (falso).





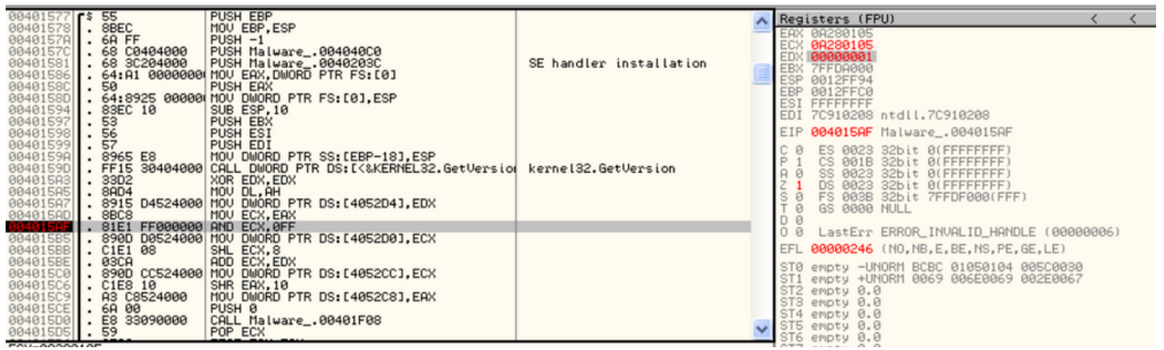
Il valore corrente di ECX è 280105
che diventa 5 dopo l’operazione logica AND
tra ECX e il valore esadecimale 0FF.

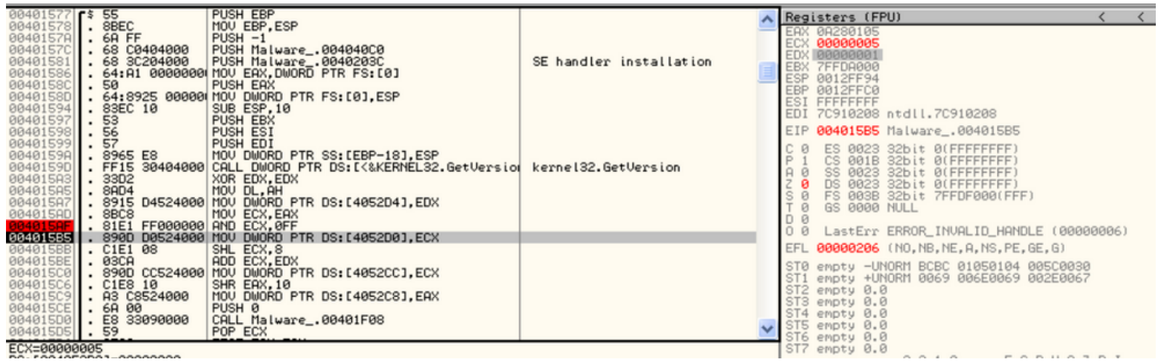
280105=00101000000000100000101

0FF=00000000000000011111111

5=00000000000000000000101

La porta logica AND, restituisce 1 quando entrambi gli ingressi sono a 1, diversamente, restituisce 0.





Il malware in questione, apre una linea di comando e richiama la libreria WS2_32.dll, che permette di creare un socket, al fine di collegarsi all’esterno della macchina. Si avvia al login in windows.
Sembrerebbe una backdoor, un attacco di tipo reverse shell.