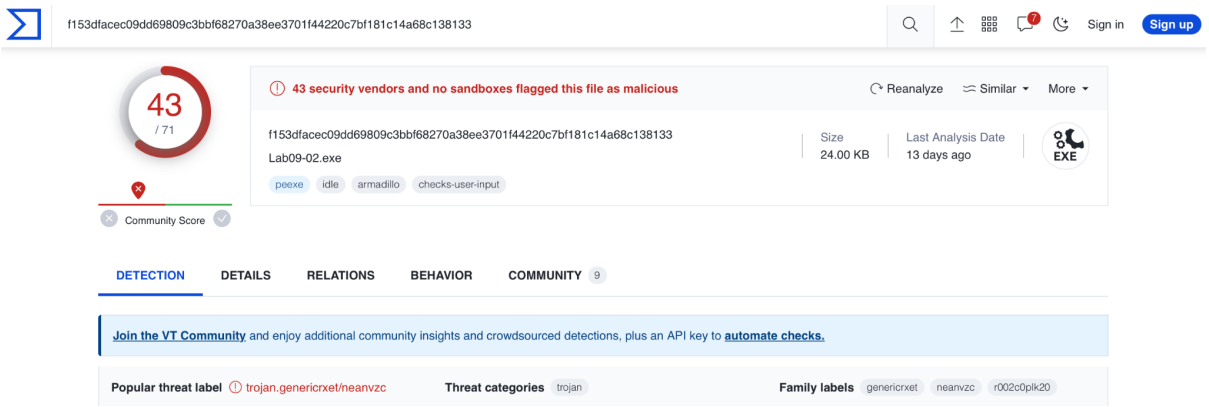
OLLY

Traccia:

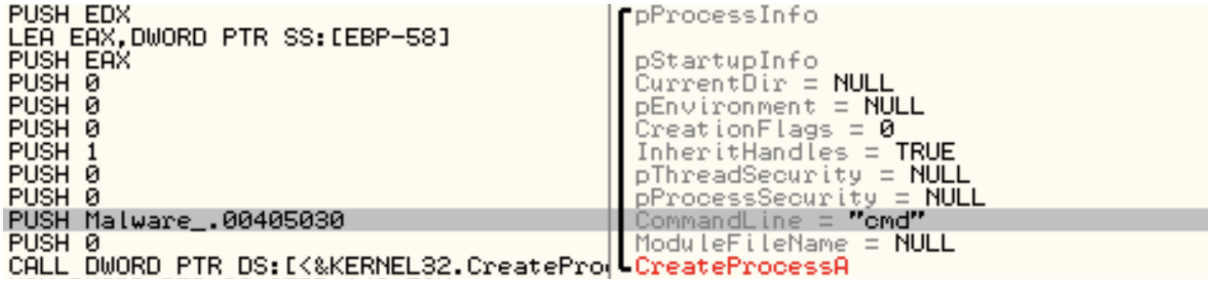
Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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

Per prima cosa effettuo una scansione dell'hash del Malware_U3_W3_L3 trovato con il software CFF Explorer



1) A questo indirizzo 0040106E il malware effettua una chiamata di funzione alla funzione "CreateProcess"



- Il valore di CommandLine è "CMD" che viene passato sullo stack utilizzando l'indirizzo 0040106E

2) Inserendo un BreakPoint software all'indirizzo 004015A3, qual'è il valore del registro EAX ?

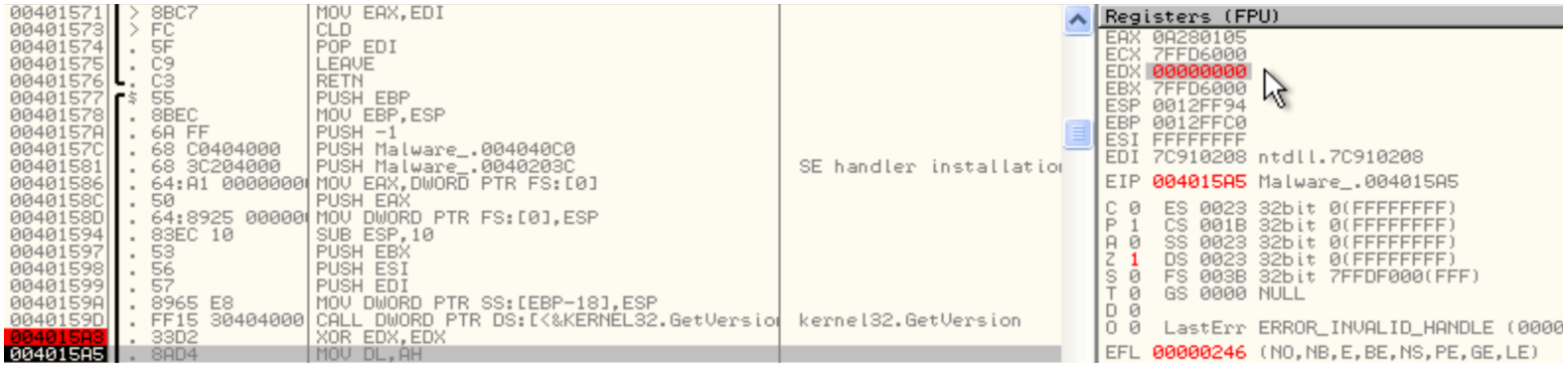
- Una volta inserito il BreakPoint sull'indirizzo 004015A3 eseguo uno Step Into e avvio

- Il valore iniziale di EDX è A28 (esadecimale)

- Eseguendo un'altro step into il valore di EDX diventerà 0 perchè l' istruzione precedente XOR a pulito lo stack

→ **EDX 00000000 è 0 in decimale**

XOR =
1 1 = 0
0 0 = 0
1 0 = 1
0 1 = 1



3) Motiva la risposta

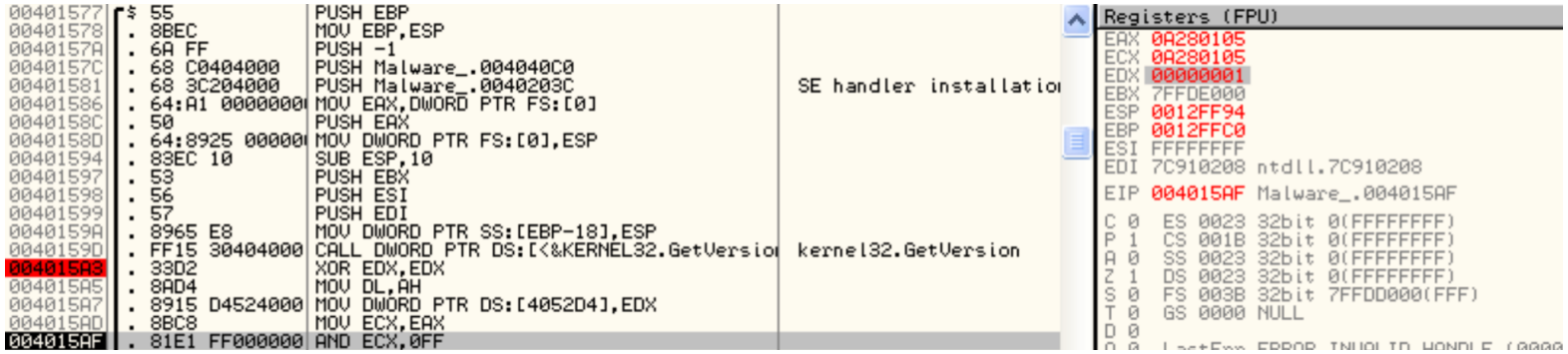
Viene eseguita l'istruzione XOR tra il registro e se stesso impostando il valore a 0

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

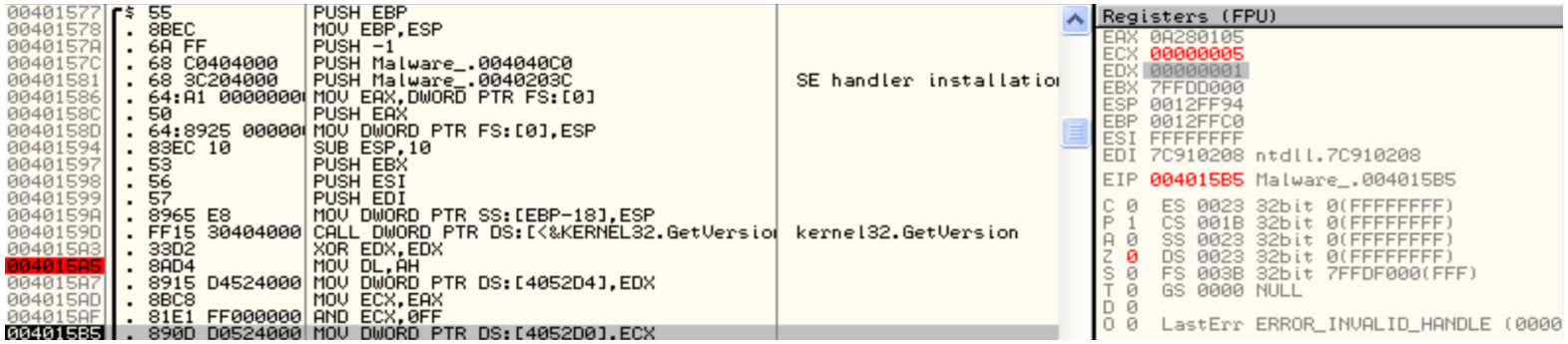
Qual è il valore del registro ECX?

Eseguite un step-into.

Qual è ora il valore di ECX ? Spiegate quale istruzione è stata eseguita



- Il valore del registro ECX è 0A280105
Dopo aver eseguito lo Step Into il valore di EDX è 5



L’istruzione che è stata eseguita è AND. Confrontando i bit dei due operandi.
Se entrambi i bit corrispondenti sono impostati a 1, il risultato sara` 1. Altrimenti, il risultato sara` 0.

Funzionamento Malware

Possiamo vedere le librerie importate in automatico da Virustotal altrimenti da CFF Explorer

Kernel32.dll

WS2_32.dll

Kernel32.dll → e` una libreria di sistema di Windows che serve per interagire con il sistema operativo. Gestisce processi, thread (flussi di esecuzione), memoria, file, tempo e risorse. Essenziale per molti programmi consentendo di eseguire operazioni tipo creare processi, leggere/scrivere file, allocare memoria e gestire il tempo di sistema.

WS2_32.dll per la programmazione del socket e le comunicazioni di rete.

Possiamo ipotizzare l'implementazione di una backdoor utilizzando:

WSASocketA per creare un socket di rete

Connect per connettersi al server remoto e inviare o ricevere comandi e dati tramite questa connessione.

Il malware in questione è una backdoor