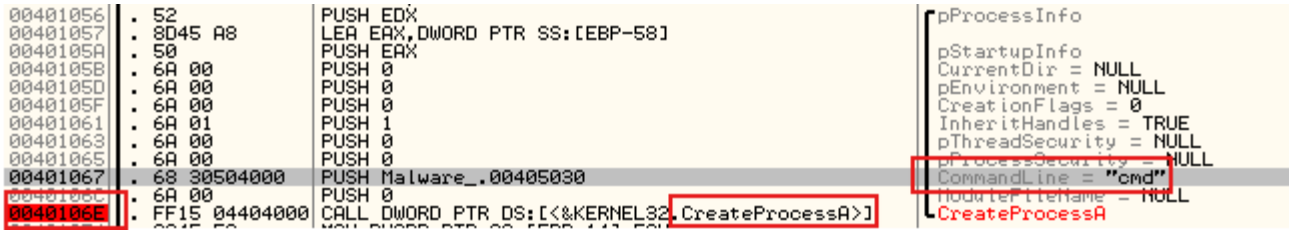
CONSEGNA U3 S11 L3

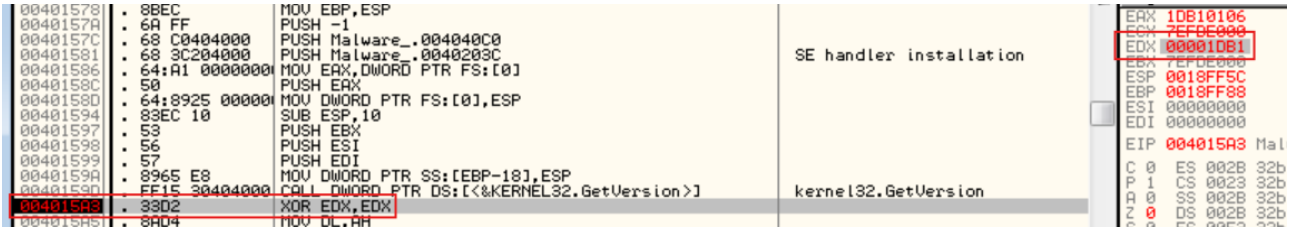
- **All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)**

Il valore del parametro che viene passato alla funzione **CreateProcess** è **"cmd".**



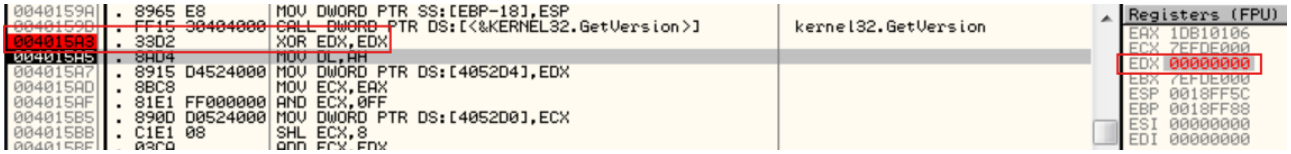
- **Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2)**

Il valore esadecimale contenuto nel registro **EDX** è **00001DB1.**



- **Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3)**

Dopo aver eseguito lo **step into** il valore di **EDX** si è azzerato.



- **Motivare la risposta (4)**

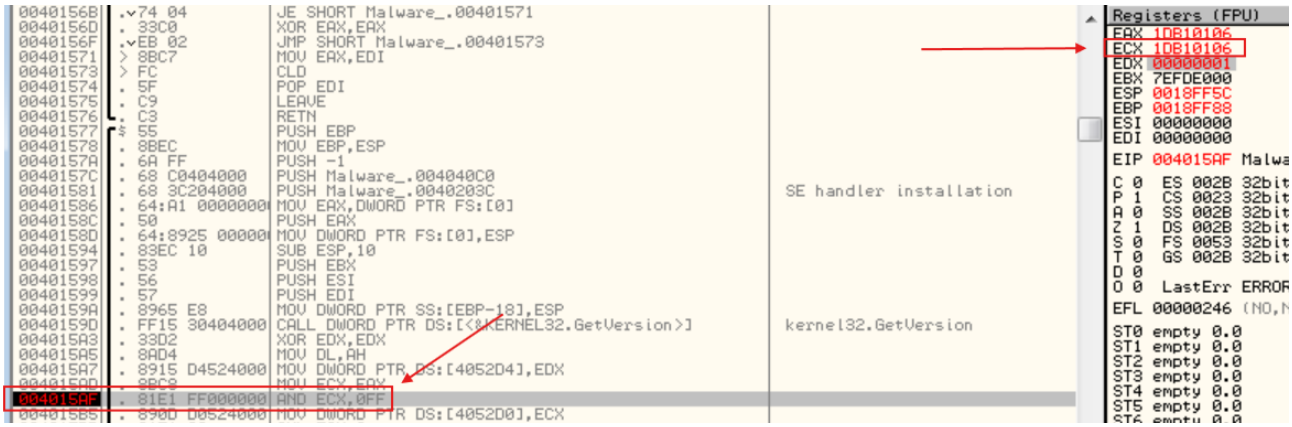
L'istruzione contrassegnata con il **breakpoint** non verrà eseguita fino a quando non si passerà oltre con l'esecuzione del codice. Effettuando lo **step-into** infatti, si riprende l'esecuzione proprio dall'istruzione contrassegnata dal **breakpoint,** che appunto modificherà il valore del registro.

- **Che istruzione è stata eseguita? (5)**

È accaduto ciò perché è stata eseguita l'operazione logica **XOR** sul registro stesso azzerandone di fatto il valore. Infatti eseguendo lo **XOR** di due valori identici essi si annullano e danno come risultato **0**.

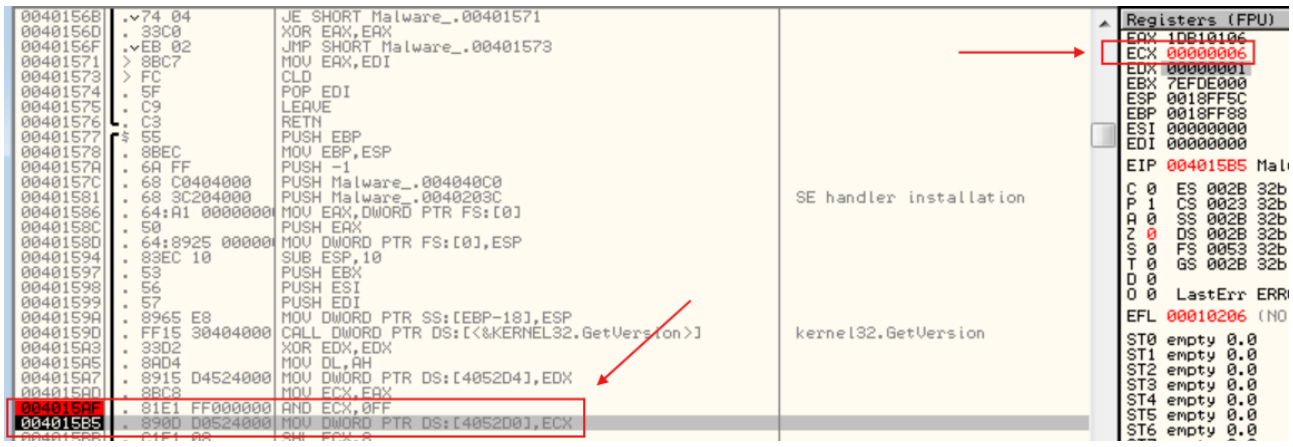
- **Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6)**

Il valore di **ECX** è **1DB10106**.



- **Eseguite uno step-into. Qual è ora il valore di ECX? (7)**

Dopo aver eseguito lo **step-into** il valore di **ECX** è cambiato in **00000006**.



- **Spiegate quale istruzione è stata eseguita (8)**

È stata eseguita l'istruzione **AND ECX, 0FF,** ovvero l'operazione **AND** tra i valori esadecimali **1DB10106** e **0FF**.

Se riportati in binario diventano rispettivamente 11101101100010000000100000110 e 11111111.

L'**AND** tra questi due valori da come risultato **110** che in esadecimale equivale al valore **6**.

- **BONUS: spiegare a grandi linee il funzionamento del malware**

Il programma malevolo effettua la chiamata di varie funzioni come quelle per la creazione di socket di rete o per ricavare gli IP di nomi di dominio. Poi esegue anche la manipolazione di file e la creazione di processi. Ci sono pure chiamate a funzioni per la manipolazione di stringhe. Di sicuro si tratta di un malware che tenta la comunicazione verso l'esterno probabilmente verso qualche dominio malevolo o infetto.