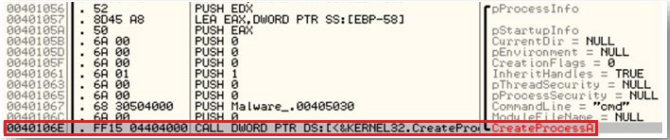
**PUNTO 1.**

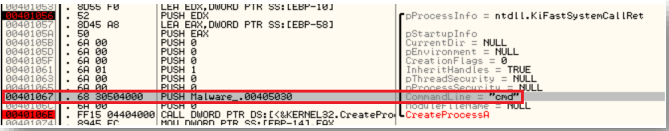
All’indirizzo di memoria “0040106E” come spiegato nella traccia troviamo una chiamata della

funzione “CreateProcess”.

Mi sposto all’indirizzo “0040106E”:

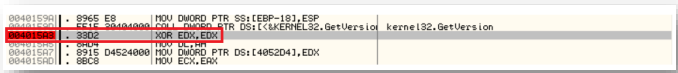


Una volta arrivati all’indirizzo possiamo notare che il valore “CommandLine” passato alla funzione sia “cmd”, ovvero il software “Prompt dei comandi“, nel sistema operativo Windows:

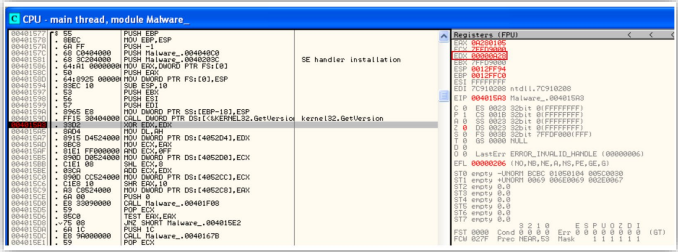


**PUNTO 2**

Inserisco un breakpoint all’indirizzo “004015A3”, utilizzando il tasto “F2”:

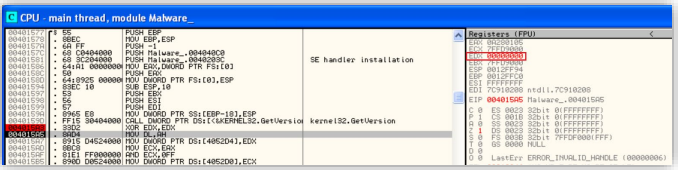


Ottengo il valore del registro EDX “00000A28”:



**PUNTI 3 E 4**

Eseguo lo step-into, utilizzando il tasto “F7” e verifico nuovamente il valore del registro EDX.



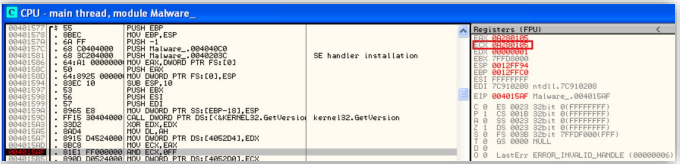
Il valore del registro è ora “0”, poiché è stato eseguito uno “XOR” dello stesso elemento. Ciò ha sempre “0” come risultato.

**PUNTO 5**

L’istruzione “XOR EDX, EDX” è stata eseguita ed ha modificato il valore del registro a 0 poiché tale istruzione equivale ad inizializzare una variabile, assegnando 0 come valore inziale.

**PUNTO 6**

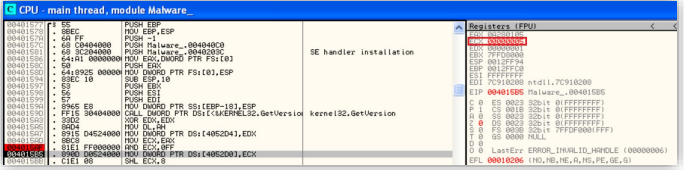
Inserisco ora un breakpoint all’indirizzo “004015AF”, di nuovo con il tasto “F2”, avvio il programma in modo da raggiungere il breakpoint e verifico il valore del registro “ECX”:



Constatiamo come il valore del registro “ECX” sia “0A280105”.

**PUNTO 7**

Eseguo ora lo step-into, di nuovo con il tasto “F7” e verifico nuovamente il valore del registro ECX.



Questa volta il valore del registro “ECX” è “00000005”

**PUNTO 8**

L’istruzione eseguita questa volta è “AND ECX, FF” ed esegue l'AND logico sul bit di EAX e del valore esadecimale 0FF