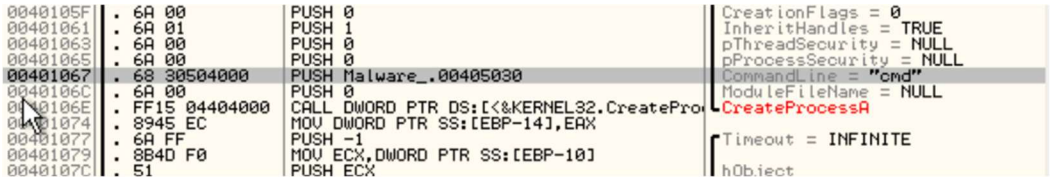
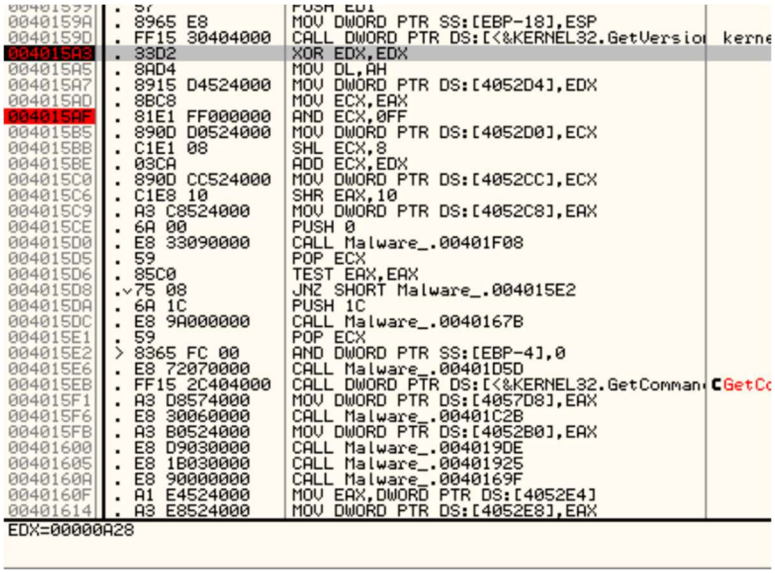
Esercizio S11-L3

All’indirizzo 0040106E il Malwareeffettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1) ⍰ Inserite un breakpointsoftware 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 breakpointall’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora alore di ECX? (7)Spiegate quale istruzione è stata eseguita (8).

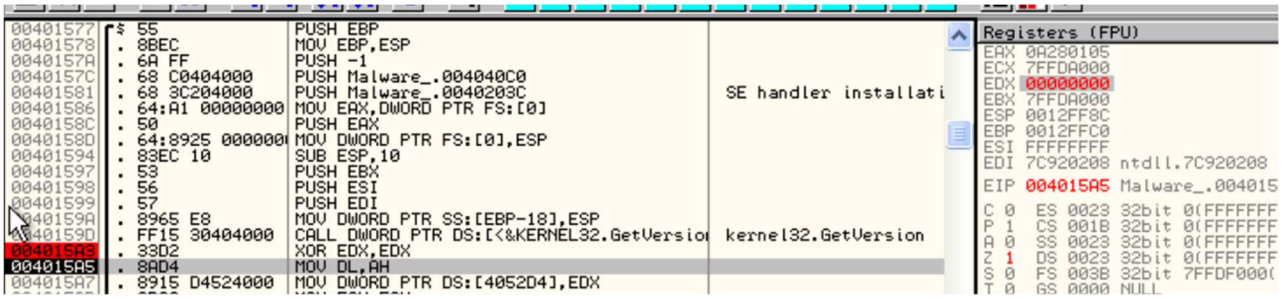
1. Il valore del parametro command line è “cmd”



2. Il valore di EDX è 00000A28

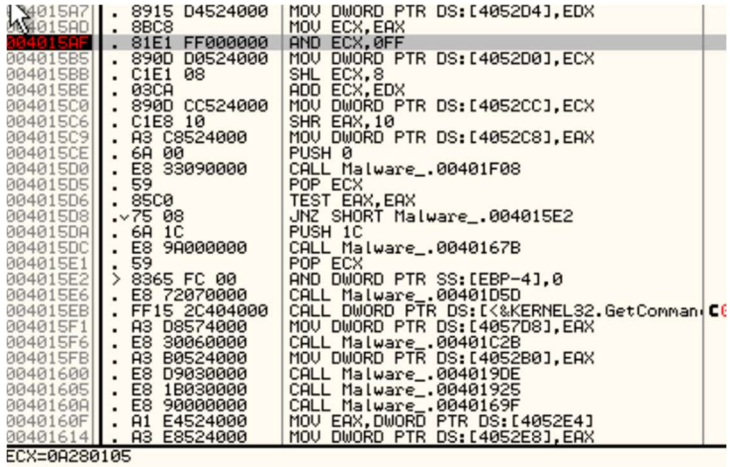


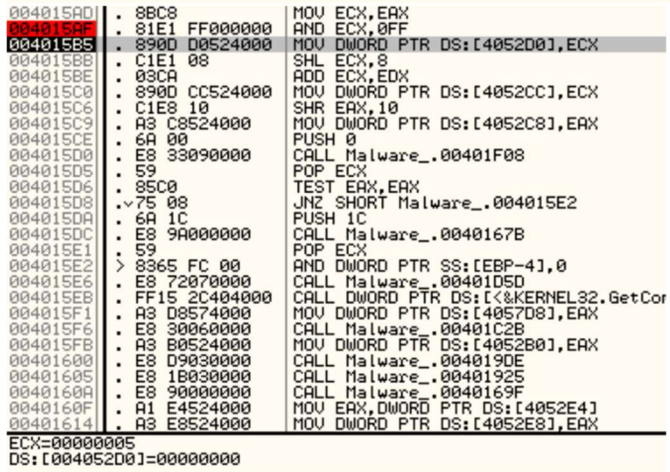
3. Dopo step into il valore di EDX è 0, a causa dell’istruzione XOR



4 Stesso procedimento di prima.

5 Il risultato di ECX dopo step into è 5, dopo l’istruzione AND che confronta i valori di ECX e 0FF che corrisponde a 256.


004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
004015E1 . 59 POP ECX
004015E2 > 8365 FC 00 AND DWORD PTR SS:[EBP-4],0
004015E6 . E8 72070000 CALL Malware_.00401D5D
004015EB . FF15 2C404000 CALL DWORD PTR DS:[<&KERNEL32.GetComman
004015F1 . A3 D8574000 MOV DWORD PTR DS:[4057D8],EAX
004015F6 . E8 30060000 CALL Malware_.00401C2B
004015FB . A3 B0524000 MOV DWORD PTR DS:[4052B0],EAX
00401600 . E8 D9030000 CALL Malware_.004019DE
00401605 . E8 1B030000 CALL Malware_.00401925
0040160A . E8 90000000 CALL Malware_.0040169F
0040160F . A1 E4524000 MOV EAX,DWORD PTR DS:[4052E4]
00401614 . A3 E8524000 MOV DWORD PTR DS:[4052E8],EAX
ECX=0A280105


004015AD . 8BC8 MOV ECX,EAX
004015AF . 81E1 FF000000 AND ECX,0FF
004015B5 . 890D D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015BB . C1E1 08 SHL ECX,8
004015BE . 03CA ADD ECX,EDX
004015C0 . 890D CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10 SHR EAX,10
004015C9 . A3 C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE . 6A 00 PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59 POP ECX
004015D6 . 85C0 TEST EAX,EAX
004015D8 .v75 08 JNZ SHORT Malware_.004015E2
004015DA . 6A 1C PUSH 1C
004015DC . E8 9A000000 CALL Malware_.0040167B
004015E1 . 59 POP ECX
004015E2 > 8365 FC 00 AND DWORD PTR SS:[EBP-4],0
004015E6 . E8 72070000 CALL Malware_.00401D5D
004015EB . FF15 2C404000 CALL DWORD PTR DS:[<&KERNEL32.GetCor
004015F1 . A3 D8574000 MOV DWORD PTR DS:[4057D8],EAX
004015F6 . E8 30060000 CALL Malware_.00401C2B
004015FB . A3 B0524000 MOV DWORD PTR DS:[4052B0],EAX
00401600 . E8 D9030000 CALL Malware_.004019DE
00401605 . E8 1B030000 CALL Malware_.00401925
0040160A . E8 90000000 CALL Malware_.0040169F
0040160F . A1 E4524000 MOV EAX,DWORD PTR DS:[4052E4]
00401614 . A3 E8524000 MOV DWORD PTR DS:[4052E8],EAX
ECX=00000005
DS:[004052D0]=00000000