Soluzione - All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «Command Line» che viene passato sullo stack? Il valore del parametro è «CMD» ovvero il command prompt di Windows, come si nota nella figura sottostante all'indirizzo 00401067

```
8D45 A8
50
6A 00
6A 00
6A 00
6A 01
6A 01
                                               LEA EAX, DWORD PTR SS: [EBP-58]
PUSH EAX
PUSH 0
PUSH 0
PUSH 0
00401057
0040105A
                                                                                                                          DStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
InheritHandles = TRUE
0040105B
0040105D
0040105F
00401061
00401063
                                               PUSH
                                                                                                                          pThreadSecurity = NULL
                     6H 00
6A 00
6B 30504000
6A 00
FF1S 04404000
894S EC
6A FF
8B4D F0
                                                                                                                         pProcessSecurity =
CommandLine = "omd"
ModuleFileName = NU
CreateProcessA
00401065
                                               PUSH
                                                                                                                                                            NULL
00401067
                                                        Malware_.00405030
                                              PUSH 0
CALL DWORD PTR DS:[<&KERNEL32.
MOV DWORD PTR SS:[EBP-14],EAX
                                                        0
DWORD PTR DS:[<&KERNEL32.CreatePro
00401060
                                                                                                                                                         NULL
0040106E
00401074
00401077
                                                                                                                          Timeout = INFINITE
                                                PUSH
00401079
                                                MOV ECX, DWORD PTR SS: [EBP-10]
                                              PUSH ECX
CALL DWORD PTR DS:[<&KERNEL32.WaitForSin
XOR EAX,EAX
MOV ESP,EBP
                                                                                                                          hOb.ject
00401070
                              00404000
                                                                                                                        WaitForSingleObject
                     33C0
8BE5
00401083
00401085
                                                POP EBP
```

Soluzione – Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita? Una volta configurato il breakpoint, clicchiamo su «play», il programma si fermerà all'istruzione XOR EDX,EDX. Prima che l'istruzione venga eseguita il valore del registro è «00000A28». Dopo lo step-into, viene eseguita l'istruzione XOR EDX,EDX che di fatto equivale ad inizializzare a zero una variabile. Quindi, dopo lo step-into il valore di EDX sarà Prima

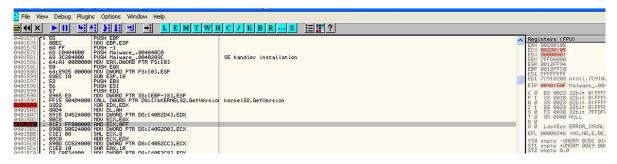


Dopo

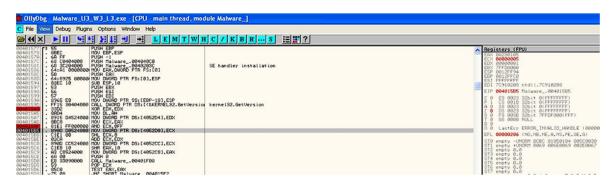


Soluzione – Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita. Configuriamo il secondo breakpoint. Il valore del registro ECX è «0A280105».

Prima



dopo lo step-into il valore del registro ECX è stato modificato in «00000005» in quanto è stata eseguita l'istruzione AND ECX, FF Dopo



Nel dettaglio, l'istruzione esegue l'AND logico sui bit di EAX e del valore esadecimale FF. Per prima cosa portiamo entrambi i valori in formato binario e poi eseguiamo l'AND logico tra i bit.

Esadecimale	Binario
0A280105	0000 1010 0010 1000 0000 0001 0000 0101
FF	0000 0000 0000 0000 0000 0000 1111 1111

Eseguendo l'AND logico tra i bit uno ad uno

0000 0000 0000 0000 0000 0000 0000 0101

Che in Esadecimale è 00000005 Ecco spiegato il valore di ECX dopo l'istruzione AND ECX, 0FF