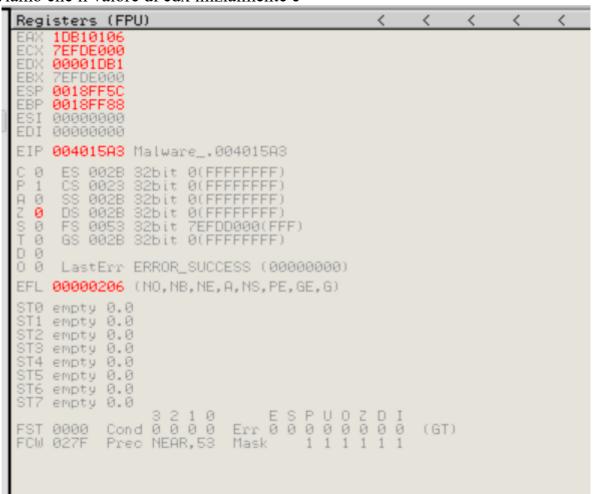
## Analisi dinamica avanzata

all'interno del malware, all'indirizzo 0040106E, troviamo il commandLine "cmd"



troviamo che il valore di edx inizialmente è



questo valore si modifica in

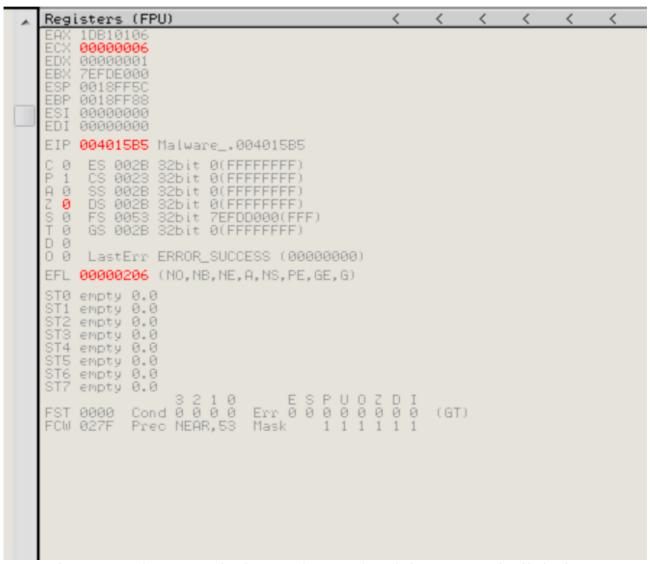
```
'EFDE000
     00000000
     7EFDE000
ESP 0018FF50
EBP 0018FF88
    00000000
    - 000000000
    004015A5 Malware_.004015A5
     ES 002B 32bit 0(FFFFFFFF)
CS 0023 32bit 0(FFFFFFFF)
SS 002B 32bit 0(FFFFFFFF)
DS 002B 32bit 0(FFFFFFFF)
FS 0053 32bit 7EFDD000(FFF)
  Ø
     GS 002B 32bit 0(FFFFFFFF)
  00
     LastErr ERROR_SUCCESS (000000000)
    00000246 (NO,NB,E,BE,NS,PE,GE,LE)
ST0 empty 0.0
 T1 empty 0.0
    empty 0.0
empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
FST 0000 Cond 0 0 0 0
                              Err 0 0 0 0 0 0 0 0
                                                             (GT)
           Pred NEAR, 53
FCW 027F
                               Mask
```

Viene modificato in 0 in quanto si utilizza l'operatore logico xor che inserisce come valore risultante 1 solo e soltanto se i due valori sono discordi e 0 se sono uguali. Dato che fa lo xor con se stesso il risultanto è sempre 0 andando così a resettare il valore a 0.

Nel indirizzo 004015AF troviamo invece questo valore di ecx

```
Registers (FPU)
        1DB10106
        000000001
        7EFDE000
 EB>
 ESP 0018FF50
 EBP 0018FF88
 ESI 00000000
 EDI 00000000
 EIP 004015AF Malware_.004015AF
        ES 002B 32bit 0(FFFFFFFF)
CS 0023 32bit 0(FFFFFFFF)
SS 002B 32bit 0(FFFFFFFF)
DS 002B 32bit 0(FFFFFFFF)
FS 0053 32bit 7EFDD000(FFF)
GS 002B 32bit 0(FFFFFFFF)
 D 0
        LastErr ERROR_SUCCESS (000000000)
 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
 ST0 empty 0.0
 ST1 empty 0.0
ST2 empty 0.0
  ST3 empty 0.0
  ST4 empty 0.0
 ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
 3210 ESPU0ZDI
FST 0000 Cond 0 0 0 Err 0 0 0 0 0 0 0
FCW 027F Prec NEAR,53 Mask 111111
                                                                           (GT)
```

E, vediamo facendo lo step-into che si modifica in



questo in quanto viene eseguita l'operazione end tra i due operatori e il risultante è 6.

a grandi linee questo malware si insinua nel registro di sistema e atraverso un socket client si collega ad un server da cui scarica virus e li va ad attivare sul computer vittima