

## Valore del parametro «CommandLine»

00401065 | . 6A 00 | PUSH 0 | pProcessSecurity | NULL  
00401067 | . 68 30504000 | PUSH Malware\_.00405030 | CommandLine | "cmd" ← Il Valore del parametro è il prompt dei comandi di Windows.  
0040106C | . 6A 00 | PUSH 0 | ModuleFileName | NULL  
0040106E | . FF15 04404000 | CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA | CreateProcessA  
00401074 | . 8945 FC | MOV DWORD PTR SS:[FRRP-141.FAX

## Primo Breakpoint

Registers (FPU)

Register	Value
EAX	0A280105
ECX	7FFDA000
EDX	00000A28
EBX	7FFDA000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208
EIP	004015A3
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
A 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FDF000(FFF)
T 0	GS 0000 NULL
D 0	
O 0	LastErr ERROR_INVALID_HANDLE

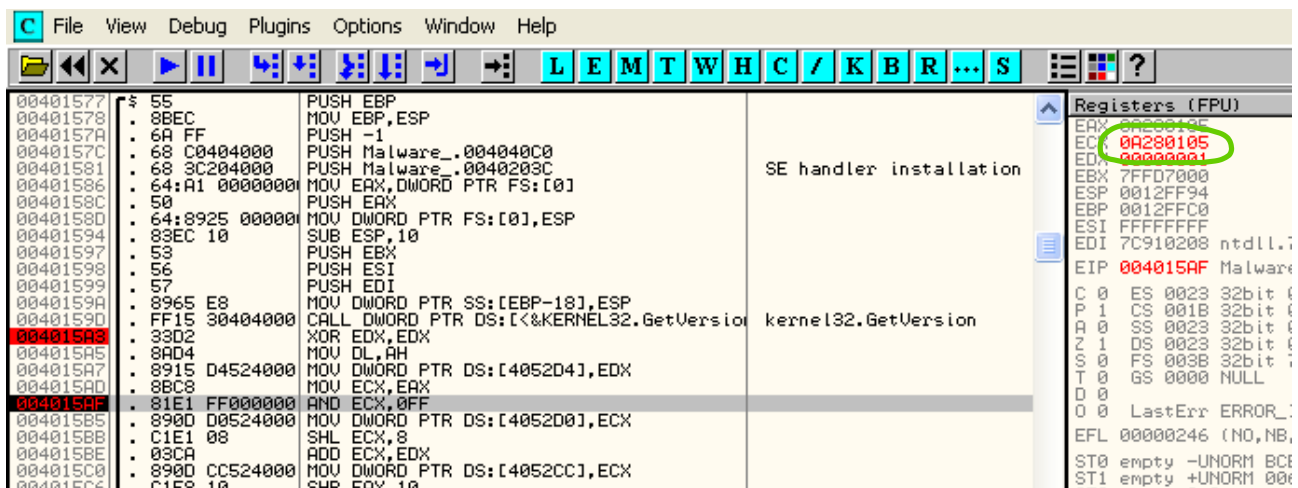
Dopo aver configurato il breakpoint e cliccando play, il programma si ferma all'indirizzo 004015A3. Il valore è 00000A28. Una volta eseguito lo step-into, il valore di EDX è uguale a 0.

Registers (FPU)

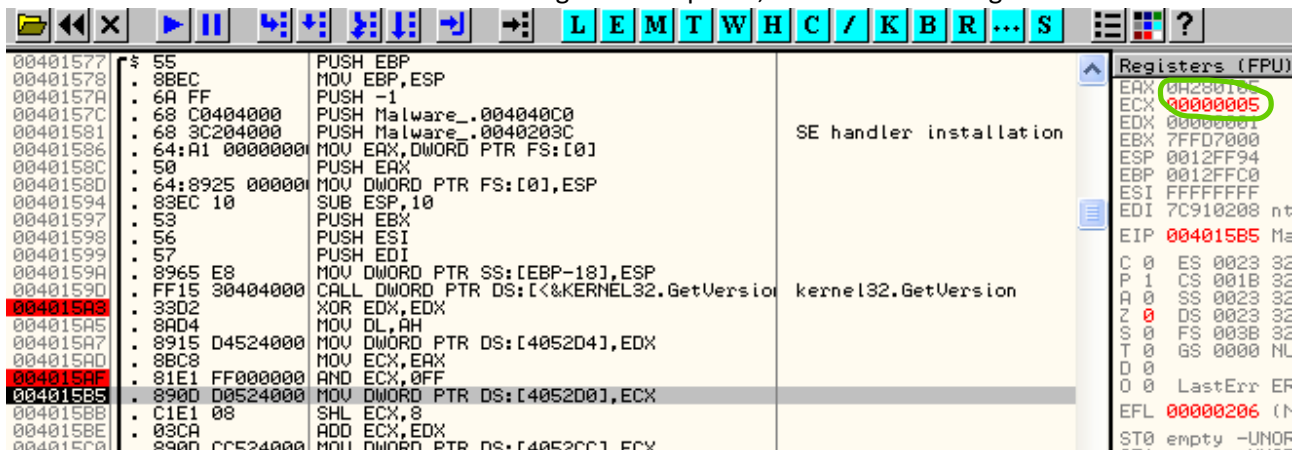
Register	Value
EAX	0A280105
ECX	7FFDA000
EDX	00000000
EBX	7FFDA000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208
EIP	004015A5
C 0	ES 0023 32b
P 1	CS 001B 32b
A 0	SS 0023 32b
Z 1	DS 0023 32b
S 0	FS 003B 32b
T 0	GS 0000 NULI
D 0	

L'istruzione eseguita è XOR EDX,EDX.

## Secondo Breakpoint



Dopo aver configurato il breakpoint e cliccando play, il programma si ferma nuovamente all'indirizzo 004015AF. Il valore è 0A280105. Una volta eseguito lo step-into, il valore di ECX è uguale a 00000005.



L'istruzione eseguita è **AND ECX,OFF.**

Enter hex number

0A280105

16

= Convert

✕ Reset

↕ Swap

Binary number (28 digits)

1010001010000000000100000101

2

Enter hex number

FF

16

= Convert

✕ Reset

↕ Swap

Binary number (8 digits)

11111111

2

Eseguendo l'AND tra i due valori otteniamo 00000000000000000000000000101 che in esadecimale è 5

## Malware

Il codice dovrebbe essere una reverse shell, dato che il cmd viene processato e rimane sempre in background. Il malware dovrebbe inizializzare la comunicazione di rete, connettendosi a un server in una determinata porta e controlla se l'operazione ha avuto successo ripetendo il loop.

Il file deve essere rinominato in **ocl** per poter essere avviato.

Il programma fa una comparazione per poter proseguire l'esecuzione. Se il file non è denominato appunto come "ocl.exe", il file si chiude.

```
CALL Malware_.00401200  
ADD ESP,8  
TEST EAX,EAX  
JE SHORT Malware_.0040124C  
MOV EAX,1  
JMP Malware_.00401206
```

Registers (FPU)		
EAX	0012FCCB	ASCII "Malware_U3_W3_L3.exe"
ECX	0012FDE0	ASCII "ocl.exe"
EDX	0012FCCB	ASCII "Malware_U3_W3_L3.exe"
EBX	7FFDE000	
ESP	0012FC6C	