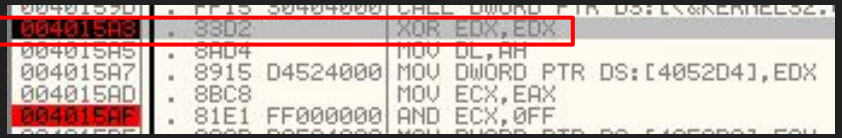
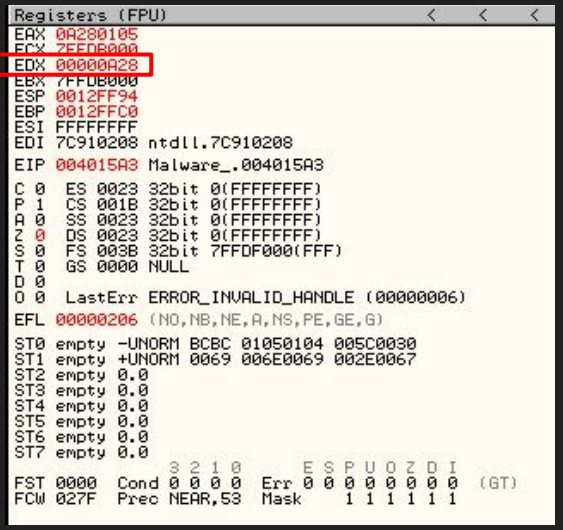
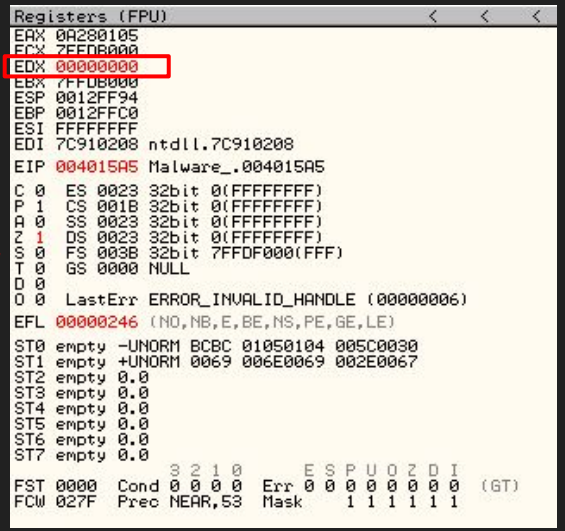
MALWARE ANALYSIS:OLLYDBG

S11 - L3

All'indirizzo 0040106E troviamo la funzione CreateProcessA. Nelle righe precedenti possiamo vedere gli argomenti preparati prima di iniziare questo processo, uno di questi è il parametro CommandLine, con il valore di cmd.







All'indirizzo 004015A3 si trova l'istruzione XOR EDX, EDX. XOR è l'istruzione e EDX è l'operando. Quando un'istruzione XOR viene eseguita da un operando a se stesso, l'operando viene "cancellato", ovvero in questo caso il registro EDX verrà cancellato e riportato a 0.

```
004015A3   . 33D2          XOR EDX,EDX
004015A5   . 8AD4          MOV DL,AH
004015A7   . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD   . 8BC8          MOV ECX,EAX
004015AF   . 81E1 FF000000 AND ECX,0FF
```

```
Registers (FPU)
EAX 00000000
ECX 0012FFB0
EDX 7C90E4F4 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFC4
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208

EIP 00401577 Malware_.<ModuleEntryPoint>

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 001B 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 1  DS 0023 32bit 0(FFFFFFFF)
S 0  FS 003B 32bit 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_INVALID_HANDLE (00000006)

EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -UNORM BCBC 01050104 005C0030
ST1 empty +UNORM 0069 006E0069 002E0067
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

```
Registers (FPU)
EAX 0A280105
ECX 00000005
EDX 00000001
EBX 7FFDE000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208

EIP 004015B5 Malware_.004015B5

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 7FFDD000(FFF)
T 0  GS 0000 NULL
D 0
O 0  LastErr ERROR_INVALID_HANDLE (00000006)

EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)

ST0 empty -UNORM BCBC 01050104 005C0030
ST1 empty +UNORM 0069 006E0069 002E0067
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0
               3 2 1 0      E S P U O Z D I
FST 0000  Cond 0 0 0 0  Err 0 0 0 0 0 0 0 0  (GT)
FCW 027F  Prec NEAR,53  Mask    1 1 1 1 1 1
```

All'indirizzo 004015F c'è l'istruzione AND EXC, OFF. In genere l'istruzione AND viene utilizzata per produrre un flag 0 o 1 a seconda che entrambi gli argomenti siano uguali, ma ha anche la capacità di cancellare i bit di un registro. Nel caso di AND EXC, OFF: OFF cancella i primi bit del registro EXC, facendolo cambiare da 0012FFB0 a 0000005.