

Valore del parametro «CommandLine»

00401065	6A 00	PUSH 0	pProcessSecurity = NULL
00401067	68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
0040106C	6A 00	PUSH 0	ModuleFileName = NULL
0040106E	FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreatePro	CreateProcessA
00401074	8945 FC	MOV DWORD PTR SS:[FAR-14],FAR	

Il Valore del parametro è il prompt dei comandi di Windows.

Primo Breakpoint

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
0040157A	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	83EC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159B	FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion	kernel32.GetVersion
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	
004015B5	89AD D4524000	MOV DWORD PTR DS:[4052D4],ECX	

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.

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
0040157A	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	83EC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159B	FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EAX	
004015B5	89AD D4524000	MOV DWORD PTR DS:[4052D4],ECX	

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

16

Binary number (28 digits)

2

Enter hex number

16

Binary number (8 digits)

2

Eseguendo l'AND tra i due valori otteniamo **0000000000000000000000000101** 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.

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

```
CALL Malware_U3_W3_L3.exe
ADD ESP,8
TEST EAX,EAX
JE SHORT Malware_.0040124C
MOV EAX,1
JMP Malware_.00401206
```

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