



S11L3

1 - Individuato l'indirizzo di memoria con la funzione CreateProcess e scoperto il valore Command Line ovvero "cmd"

. 6A 00	PUSH 0	CurrentDir = NULL
. 6A 00	PUSH 0	pEnvironment = NULL
. 6A 00	PUSH 0	CreationFlags = 0
. 6A 01	PUSH 1	InheritHandles = TRUE
. 6A 00	PUSH 0	pThreadSecurity = NULL
. 6A 00	PUSH 0	pProcessSecurity = NULL
. 68 30504000	PUSH Malware_.00405030	CommandLine = "cmd"
. 6A 00	PUSH 0	ModuleFileName = NULL
. FF15 04404000	CALL DWORD PTR DS:[&KERNEL32.CreateProcessA]	CreateProcessA
. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
. 6A FF	PUSH -1	Timeout = INFINITE
. 0B4D EA	MOV ECX,DWORD PTR SS:[EBP-10]	

Valore del registro EDX prima del BreakPoint

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	
0040159D	. 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	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	

Registers (FPU)
EAX 0A280105
ECX 7FFDA000
EDX 00000A28
EBX 7FFDA000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C920208
EIP 004015A3
C 0 ES 0023
P 1 CS 001B

Valore del registro EDX dopo il BreakPoint

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	
0040159D	. 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	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015BB	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	

Registers (FPU)
EAX 0A280105
ECX 7FFDA000
EDX 00000000
EBX 7FFDA000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C920208
EIP 004015A5
C 0 ES 0023
P 1 CS 001B
A 0 SS 0023
Z 1 DS 0023

**Notiamo che il valore del
registro dopo il BP è 0. Questo
perchè passa attraverso
l'istruzione XOR EDX,EDX che
restituisce 0 quando i due
operandi sono uguali**

Settato il BP all'indirizzo richiesto e individuato il valore del registro ECX

00401580	. 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	
0040159D	. 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	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	

Registers (FPU)
EAX 0A280105
ECX 0A280105
EDX 00000001
EBX 7FFDA000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C920208 ntdll
EIP 004015AF Malicious
C 0 ES 0023 32b
P 1 CS 001B 32b
A 0 SS 0023 32b

Eseguito lo step info e visualizzato il valore del registro ECX che risulta 05

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	
0040159D	. 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	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	

Registers (FPU)
EAX 0A280105
ECX 00000005
EDX 00000001
EBX 7FFDA000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C920208 ntdll
EIP 004015B5 Malicious
C 0 ES 0023 32b
P 1 CS 001B 32b
A 0 SS 0023 32b
Z 0 DS 0023 32b
S 0 FS 003B 32b
T 0 GS 0000 NUL

**Notiamo che il valore del registro ECX
cambia in 5 che è il risultato dopo
l'istruzione AND ECX, 0FFh che esegue un
operazione tra i due operandi**

**Bonus; Attraverso le funzioni
WSASocket, Connect, HTONS,
GETHOSTBYNAME, CLOSESOCKET si
potrebbe pensare che la funzione del
Malware è quella di connettersi ed
aprire un socket che resti in ascolto**