

CONSEGNA U3 S11 L3

- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)

Il valore del parametro che viene passato alla funzione **CreateProcess** è **"cmd"**.

00401056	. 52	PUSH EDI	
00401057	. 8D45 A8	LEA EAX, DWORD PTR SS:[EBP-58]	pProcessInfo
0040105A	. 50	PUSH EAX	pStartupInfo
0040105B	. 6A 00	PUSH 0	CurrentDir = NULL
0040105D	. 6A 00	PUSH 0	pEnvironment = NULL
0040105F	. 6A 00	PUSH 0	CreationFlags = 0
00401061	. 6A 01	PUSH 1	InheritHandles = TRUE
00401063	. 6A 00	PUSH 0	pThreadSecurity = NULL
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.CreateProcessA>]	CreateProcessA

- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2)

Il valore esadecimale contenuto nel registro **EDX** è **00001DB1**.

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]	SE handler installation
0040158C	. 50	PUSH EAX	
0040158D	. 64:8925 00000000	MOV DWORD PTR FS:[0], ESP	
00401594	. 8BEC 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	

- Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3)

Dopo aver eseguito lo **step into** il valore di **EDX** si è azzerato.

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 04524000	MOV DWORD PTR DS:[4052D4], EDX	
004015AD	. 8BC8	MOV ECX, EAX	
004015AF	. 81E1 FF000000	AND ECX, 0FF	
004015B5	. 89D0 00524000	MOV DWORD PTR DS:[4052D0], ECX	
004015BB	. C1E1 08	SHL ECX, 8	
004015BF	. 8AFA	MOV AL, FFA	

- Motivare la risposta (4)

L'istruzione contrassegnata con il **breakpoint** non verrà eseguita fino a quando non si passerà oltre con l'esecuzione del codice. Effettuando lo **step-into** infatti, si riprende l'esecuzione proprio dall'istruzione contrassegnata dal **breakpoint**, che appunto modificherà il valore del registro.

- Che istruzione è stata eseguita? (5)

È accaduto ciò perché è stata eseguita l'operazione logica **XOR** sul registro stesso azzerandone di fatto il valore. Infatti eseguendo lo **XOR** di due valori identici essi si annullano e danno come risultato **0**.

- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6)

Il valore di **ECX** è **1DB10106**.

- Eseguite uno step-into. Qual è ora il valore di ECX? (7)

Dopo aver eseguito lo **step-into** il valore di **ECX** è cambiato in **00000006**.

- Spiegate quale istruzione è stata eseguita (8)

È stata eseguita l'istruzione **AND ECX, 0FF**, ovvero l'operazione **AND** tra i valori esadecimali **1DB10106** e **0FF**.

Se riportati in binario diventano rispettivamente 11101101100010000000100000110 e 11111111.

L'**AND** tra questi due valori dà come risultato **110** che in esadecimale equivale al valore **6**.

- **BONUS: spiegare a grandi linee il funzionamento del malware**

Il programma malevolo effettua la chiamata di varie funzioni come quelle per la creazione di socket di rete o per ricavare gli IP di nomi di dominio. Poi esegue anche la manipolazione di file e la creazione di processi. Ci sono pure chiamate a funzioni per la manipolazione di stringhe. Di sicuro si tratta di un malware che tenta la comunicazione verso l'esterno probabilmente verso qualche dominio malevolo o infetto.