

Pratica 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?

Il valore del parametro è CMD ovvero il command prompt di Windows.

0040105D	. 6A 00	PUSH 0	Environment = 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
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	Timeout = INFINITE
00401077	. 6A FF	PUSH -1	hObject
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	WaitForSingleObject
0040107C	. 51	PUSH ECX	
0040107D	. FF15 00404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSingleObject]	

- Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Dopo aver impostato il breakpoint, faccio partire il programma. Si fermerà quando raggiunge l'istruzione XOR EDX, EDX. Prima dell'esecuzione di questa istruzione, **il valore di EDX è "00000A28"**.

00401577	. 55	PUSH EBP	
00401578	. 8BEC	MOV EBP,ESP	
00401579	. 6A FF	PUSH -1	
0040157C	. 68 00404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	
00401586	. 64:01 00000000	MOV EDI,DWORD PTR FS:[0]	
0040158C	. 50	PUSH EAX	
00401590	. 64:8925 000000	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	. 80DA	MOV DL,AH	
004015A7	. 891E D4524000	MOV DWORD PTR DS:[4052D4],EDX	

Dopo aver eseguito lo step-into, **l'istruzione XOR EDX, EDX** azzerà il valore di EDX, che

00401577	. 55	PUSH EBP	
00401578	. 8BEC	MOV EBP,ESP	
00401579	. 6A FF	PUSH -1	
0040157C	. 68 00404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	
00401586	. 64:01 00000000	MOV EDI,DWORD PTR FS:[0]	
0040158C	. 50	PUSH EAX	
00401590	. 64:8925 000000	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	. 80DA	MOV DL,AH	
004015A7	. 891E D4524000	MOV DWORD PTR DS:[4052D4],EDX	

diventa quindi 0.

- Inserite un secondo breakpointall'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV ESP, EBP	
00401579	PUSH -1	
0040157C	PUSH Malware_.004040C0	
00401581	PUSH Malware_.0040203C	
00401586	MOV EAX, DWORD PTR FS:[0]	
0040158C	PUSH EAX	
00401590	MOV DWORD PTR FS:[0], ESP	
00401594	SUB ESP, 10	
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-10], ESP	
0040159D	CALL DWORD PTR DS:[4&KERNEL32.GetVersion	kernel32.GetVersion
004015A2	XOR EDX, EDX	
004015A3	MOV DL, AH	
004015A7	MOV DWORD PTR DS:[4052D41], EDX	
004015AD	MOV ECX, EAX	
004015B0	AND ECX, 0FF	
004015B5	MOV DWORD PTR DS:[4052D01], ECX	
004015B8	SHL ECX, 8	
004015BB	ADD ECX, EDX	
004015C0	MOV DWORD PTR DS:[4052CC1], ECX	
004015C8	AND ECX, 00000005	
004015D0	MOV DWORD PTR DS:[4052C01], EDI	

Register	Value
EAX	00280105
ECX	00280105
EDX	00000001
ESP	7FFD0000
EBP	0012FF34
ESI	FFFFFFFF
EDI	7C910208
EIP	004015C8
EFLAGS	00000246
CS	001B
DS	0023
SS	0023
FS	003B
GS	0000
IOPL	0
LastError	ERROR_INVALID_HANDLE

Il valore del registro ECX è «0A280105»,
 Dopo aver eseguito lo step-into, il valore del registro ECX è cambiato in "00000005"
 perché è stata eseguita l'istruzione **AND ECX, FF**, la quale effettua un'operazione logica

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV ESP, EBP	
00401579	PUSH -1	
0040157C	PUSH Malware_.004040C0	
00401581	PUSH Malware_.0040203C	
00401586	MOV EAX, DWORD PTR FS:[0]	
0040158C	PUSH EAX	
00401590	MOV DWORD PTR FS:[0], ESP	
00401594	SUB ESP, 10	
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-10], ESP	
0040159D	CALL DWORD PTR DS:[4&KERNEL32.GetVersion	kernel32.GetVersion
004015A2	XOR EDX, EDX	
004015A3	MOV DL, AH	
004015A7	MOV DWORD PTR DS:[4052D41], EDX	
004015AD	MOV ECX, EAX	
004015B0	AND ECX, 0FF	
004015B5	MOV DWORD PTR DS:[4052D01], ECX	
004015B8	SHL ECX, 8	
004015BB	ADD ECX, EDX	
004015C0	MOV DWORD PTR DS:[4052CC1], ECX	
004015C8	AND ECX, 00000005	
004015D0	MOV DWORD PTR DS:[4052C01], EDI	

Register	Value
EAX	00280105
ECX	00000005
EDX	00000001
ESP	7FFD0000
EBP	0012FF34
ESI	FFFFFFFF
EDI	7C910208
EIP	004015B5
EFLAGS	00000206
CS	001B
DS	0023
SS	0023
FS	003B
GS	0000
IOPL	0
LastError	ERROR_INVALID_HANDLE

tra il valore corrente di ECX e "FF".