

Pratica S11/L3

Giaimo Rosario

Traccia:

Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3 sul desktop della macchina virtuale dedicata all'analisi del malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).
- BONUS: spiegare a grandi linee il funzionamento del malware

Svolgimento

- 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)

0040105F	6A 00	PUSH 0	
00401061	6A 01	PUSH 1	
00401063	6A 00	PUSH 0	
00401065	6A 00	PUSH 0	
00401067	68 30504000	PUSH Malware_.00405030	ASCII "cmd"
0040106C	6A 00	PUSH 0	
0040106E	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA	kernel32.CreateProcessA
00401074	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
00401077	6A FF	PUSH -1	
00401079	8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	
0040107C	51	PUSH ECX	
0040107D	FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSingleObject	kernel32.WaitForSingleObject
00401083	33C0	XOR EAX,EAX	
00401085	8BE5	MOV ESP,EBP	
00401087	5D	POP EBP	
00401088	C3	RETN	
00401089	55	PUSH EBP	
0040108A	8BEC	MOV EBP,ESP	
0040108C	81EC 00010000	SUB ESP,100	

Il valore del parametro è "CMD"

- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)

Il valore del registro EDX è 00401577

PRIMA

Debugger window showing assembly code and registers. The assembly window displays instructions from 00401577 to 004015F0. The registers window shows the state of registers including EAX, ECX, EDI, and EIP. The instruction at 00401577 is 'PUSH EBP'.

DOPO

Debugger window showing assembly code and registers. The assembly window displays instructions from 00401577 to 004015F0. The registers window shows the state of registers including EAX, ECX, EDI, and EIP. The instruction at 00401577 is 'PUSH EBP'.

- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

PRIMA

Debugger window showing assembly code and registers. The assembly window displays instructions from 00401577 to 004015F0. The registers window shows the state of registers including EAX, ECX, EDI, and EIP. The instruction at 00401577 is 'PUSH EBP'.

DOPO

Debugger window showing assembly code and registers. The assembly window displays instructions from 00401577 to 004015F0. The registers window shows the state of registers including EAX, ECX, EDI, and EIP. The instruction at 00401577 is 'PUSH EBP'.

- BONUS: spiegare a grandi linee il funzionamento del malware

Dall'analisi che ho effettuato la minaccia in questione potrebbe essere un Trojan, ma è probabile che si tratti di uno Spyware.