

Esercizio S11 L3

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 dei 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?

00401050	. 894D E4	MOV DWORD PTR SS:[EBP-1C],ECX	
00401053	. 8D55 F0	LEA EDX,DWORD PTR SS:[EBP-10]	
00401056	. 52	PUSH EDX	
00401057	. 8D45 A8	LEA EAX,DWORD PTR SS:[EBP-58]	
0040105A	. 50	PUSH EAX	
0040105B	. 6A 00	PUSH 0	
0040105D	. 6A 00	PUSH 0	
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	
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA]	
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

pProcessInfo

pStartupInfo

CurrentDir = NULL

pEnvironment = NULL

CreationFlags = 0

InheritHandles = TRUE

pThreadSecurity = NULL

pProcessSecurity = NULL

CommandLine = "cmd"

ModuleFileName = NULL

Il valore del parametro CommandiLine è: **cmd**

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

00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159B	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
0040159C	3302	XOR EDX,EDX	
0040159D	8004	MOV DL,4H	
004015A7	915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A8	8BC8	MOV ECX,ERX	
004015A9	91E1 FF000000	AND ECX,0FF	
004015AB	990 D0524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B5	C1E1 08	SHL ECX,8	
004015B6	830A	ADD ECX,EDX	
004015B7	990 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	C1E8 10	SHR ERX,10	
004015C9	A3 C8524000	MOV DWORD PTR DS:[4052C8],ERX	
004015CE	6A 00	PUSH 0	
004015D0	E8 38090000	CALL Malware_.00401F08	

Registers (FPU)	
EAX	0A280105
ECX	77F00000
EDX	00000000
EBX	77F00000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015A3 Malware_.004015A3
C 0	ES 0023 32bit 0(FFFFFFFF)
P 1	CS 001B 32bit 0(FFFFFFFF)
D 0	SS 0023 32bit 0(FFFFFFFF)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 77FDF000(FFF)
G 0	GS 0000 NULL

Il valore del registro EDX è **00000A28**

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159B	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
0040159C	3302	XOR EDX,EDX	
0040159D	8004	MOV DL,4H	
004015A7	915 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A8	8BC8	MOV ECX,ERX	
004015A9	91E1 FF000000	AND ECX,0FF	
004015AB	990 D0524000	MOV DWORD PTR DS:[4052D0],ECX	

Registers (FPU)	
EAX	0A280105
ECX	77F00000
EDX	00000000
EBX	77F00000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015A5 Malware_.004015A5

Il valore del registro EDX ora è **00000000**. Lo step into viene utilizzato per esaminare righe di codice e a fronte di una chiamata di funzione accedere alla sua implementazione. In questo caso viene eseguita la riga di codice **XOR EDX, EDX** che è il comando per azzerare un registro.

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



Address	Disassembly	Comment
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-10],ESP	
0040159B	CALL DWORD PTR DS:[<&kernel32.GetVersion	kernel32.GetVersion
0040159C	XOR EDX,EDX	
0040159D	MOV DL,AH	
0040159E	MOV DWORD PTR DS:[4052D4],EDX	
0040159F	MOV ECX,ERX	
004015A0	AND ECX,0FF	
004015A1	MOV DWORD PTR DS:[4052D0],ECX	

Register	Value
EAX	00000000
ECX	0A280105
EDX	00000000
EBX	7FFD8000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015AF Malware_.004015AF

Il valore del registro ECX è **0A280105**.

Eseguite un step-into. Qual è ora il valore di ECX?
Spiegate quale istruzione è stata eseguita.



Address	Disassembly	Comment
00401597	PUSH EBX	
00401598	PUSH ESI	
00401599	PUSH EDI	
0040159A	MOV DWORD PTR SS:[EBP-10],ESP	
0040159B	CALL DWORD PTR DS:[<&kernel32.GetVersion	kernel32.GetVersion
0040159C	XOR EDX,EDX	
0040159D	MOV DL,AH	
0040159E	MOV DWORD PTR DS:[4052D4],EDX	
0040159F	MOV ECX,ERX	
004015A0	AND ECX,0FF	
004015A1	MOV DWORD PTR DS:[4052D0],ECX	

Register	Value
EAX	00000000
ECX	00000005
EDX	00000000
EBX	7FFD8000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208 ntdll.7C910208
EIP	004015B5 Malware_.004015B5

Il valore di ECX è di **00000005** questo perchè viene eseguita una istruzione **AND** tra il registro ECX con valore 0A280105 e il valore **0FF** scritto in esadecimale. Il risultato di tale operazione è appunto 00000005.

BONUS: spiegare a grandi linee il funzionamento del malware.

Analizzando il comportamento del malware notiamo che crea processi in windows, crea file, prova ad nascondersi da strumenti di analisi, crea e si connette a TCP socket inoltre si comporta come un TCP client. Quindi potrebbe essere una reverse shell.