

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?

Inserite un breakpoint software 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?

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

BONUS: spiegare a grandi linee il funzionamento del malware

Qual è il valore del parametro «CommandLine» che viene passato sullo stack?

00401056	. 52	PUSH EDI	pProcessInfo
00401057	. 8D45 A8	LEA EAX, DWORD PTR SS:[EBP-58]	pStartupInfo
0040105A	. 50	PUSH EAX	CurrentDir = NULL
0040105B	. 6A 00	PUSH 0	pEnvironment = NULL
0040105D	. 6A 00	PUSH 0	CreationFlags = 0
0040105F	. 6A 00	PUSH 0	InheritHandles = TRUE
00401061	. 6A 01	PUSH 1	pThreadSecurity = NULL
00401063	. 6A 00	PUSH 0	pProcessSecurity = NULL
00401065	. 6A 00	PUSH 0	CommandLine = "cmd"
00401067	. 68 30504000	PUSH Malware_.00405030	ModuleFileName = NULL
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreateProcessA]	CreateProcessA

Come vediamo da OllyDBG il valore del parametro **CommandLine** che viene passato sullo stack a seguito della chiamata alla funzione è **cmd**.

Inserite un breakpoint software 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.

00401598	. 56	PUSH ESI		EAX 7FFD5000
00401599	. 57	PUSH EDI		EDX 00000A28
0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP		EBX 7FFD5000
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion	ESP 0012FF94
004015A3	. 33D2	XOR EDX,EDX		EBP 0012FFC0
004015A4	. 5B	POP EBX		ESI FFFFFFFF

Una volta impostato il **breakpoint** all' indirizzo di memoria **004015A3** posso andare a verificare il valore del registro **EDX** nella tabella dei registri. Come si vede dallo screenshot, questo valore è **00000A28**.

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

00401599	. 57	PUSH EDI		EAX 04280105
0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP		ECX 7FFDB000
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion	EDX 00000000
004015A3	. 33D2	XOR EDX,EDX		EBX 7FFDB000
004015A5	. 8AD4	MOV DL,AH		ESP 0012FF94
				EBP 0012FFC0

Una volta eseguito lo **step-into**, vediamo come il valore del registro **EDX** sia cambiato in **00000000**.

Attraverso lo step-into viene eseguita l'istruzione **XOR** che è equivalente ad inizializzare a **0** una variabile. L'istruzione che viene eseguita, nello specifico, è **XOR EDX, EDX**.

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

004015A5	. 8AD4	MOV DL,AH		EAX	0A280105
004015A7	. 8915 04524000	MOV DWORD PTR DS:[4052D4],EDX		ECX	0A280105
004015AD	. 8BC8	MOV ECX,EAX		EDX	00000001
004015AF	. 81E1 FF000000	AND ECX,0FF			

Dopo aver impostato un nuovo breakpoint sull' indirizzo **004015AF** , vediamo come il valore del registro **ECX** sia **0A280105**.

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

004015AD	. 8BC8	MOV ECX,EAX		EAX	0A280105
004015AF	. 81E1 FF000000	AND ECX,0FF		ECX	00000005
004015B5	. 8900 00524000	MOV DWORD PTR DS:[4052D0],ECX		EDX	00000001
004015BB	. C1F1 08	SHL ECX,8			

Dopo aver eseguito lo step-into, il valore del registro **ECX** cambia in **00000005**

Questo è il risultato dell' esecuzione dell' istruzione **AND** sui bit nel registro **ECX** ed il valore esadecimale **000000FF**.

BONUS: spiegare a grandi linee il funzionamento del malware

Dopo aver ricavato l'hash del file eseguibile tramite il tool **md5deep** ed averlo analizzato con Virus Total, è venuto fuori che il malware sembrerebbe essere un **Trojan**.