

# OLLYDBG

Pablo Andres Balbuena Rios

# 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 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? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) 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 un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
- BONUS: spiegare a grandi linee il funzionamento del malware

# Traccia 1

00401053	. 8D55 F0	LEA EDX,DWORD PTR SS:[EBP-10]	pProcessInfo pStartupInfo CurrentDir = NULL pEnvironment = NULL CreationFlags = 0 InheritHandles = TRUE pThreadSecurity = NULL pProcessSecurity = NULL CommandLine = "cmd" ModuleFileName = NULL
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	CreateProcessA
0040106C	. 6A 00	PUSH 0	
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	

Il valore del parametro è : cmd

# Traccia 2

Il valore di EDX  
è: 00401577

Si esegue l'istruzione  
di XOR del valore di  
EDX, ovvero si azzerà il  
suo valore.

Il valore di  
EDX è: 00000000

Registers (FPU)			<
EAX	771933B8	kernel32.BaseThreadInitThunk	
ECX	00000000		
EDX	00401577	Malware_.<ModuleEntryPoint>	
EBX	7EFDE000		
ESP	0018FF84		
EBP	0018FF88		
ESI	00000000		
EDI	00000000		

004015A3		. 33D2		XOR EDX,EDX
----------	--	--------	--	-------------

Registers (FPU)			<
EAX	771933B8	kernel32.BaseThreadInitThunk	
ECX	00000000		
EDX	00000000		
EBX	7EFDE000		
ESP	0018FF84		
EBP	0018FF88		
ESI	00000000		
EDI	00000000		

# Traccia 3

Il valore di ECX è:  
771933B8

Si esegue AND tra il  
valore di ECX ed il  
numero 0FF "255".

Il valore di ECX è:  
000000B8

Registers (FPU)			<
EAX	771933B8	kernel32.BaseThreadInitThunk	
ECX	771933B8	kernel32.BaseThreadInitThunk	
EDX	00000033		
EBX	7EFDE000		
ESP	0018FF84		
EBP	0018FF88		
ESI	00000000		
EDI	00000000		
EIP	004015AF	Malware_.004015AF	

004015AF | . 81E1 FF000000 | AND ECX,0FF

Registers (FPU)			<
EAX	771933B8	kernel32.BaseThreadInitThunk	
ECX	000000B8		
EDX	00000033		
EBX	7EFDE000		
ESP	0018FF84		
EBP	0018FF88		
ESI	00000000		
EDI	00000000		
EIP	004015B5	Malware_.004015B5	