

## ANALISI DINAMICA AVANZATA CON 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 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.

Nell'esercizio di oggi procediamo con un'analisi dinamica avanzata di un malware tramite il tool OllyDBG.

Il primo quesito richiede si identificare il valore del parametro CommandLine alla chiamata della funzione "CreateProcess". Con OllyDBG ci spostiamo sull'indirizzo di chiamata della funzione e diamo un'occhiata ai push sullo stack che la precedono. Vediamo che il parametro "CommandLIne" assume il valore di "cmd". Ciò significa che quando viene inserito il comando "cmd" veà inserito il codice malevolo.

```
00401050: 8D55 F0    LEA EDX,DWORD PTR SS:[EBP-10]
00401055: 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 B1        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.CreateProc
0040106E] pCreateInfo
pStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
InheritHandles = TRUE
pThreadSecurity = NULL
pProcessSecurity = NULL
CommandLine = "cmd"
ModuleFileName = NULL
CreateProcessA
```

Ci spostiamo alla locazione di memoria 004015A3 e inseriamo qui un breakpoint. Il valore del registro EDX a questo punto è 00000A28 (in decimale 2.600).

Registers (FPU)	
EAX	00280105
ECX	7FFDC000
EDX	00000A28
EBX	7FFDC000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C920208 ntdll.7C920208
EIP	004015A3 Malware_.004015A3

Procedendo con lo step-into, il valore di EDX cambierà a 0, in quanto alla locazione 004015A3 avviene un'opeazione logia XOR tra EDX e se stesso; in questi casi il risultato è sempre 0.

00000A28 = 101000101000

101000101000	XOR
101000101000	
000000000000	0

0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	EAX 0A280105
0040159D	. FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	ECX 7FFDC000
004015A3	. 3B02	XOR EDX,EDX	EDX 00000000
004015A5	. 8AD4	MOV DL,AH	EBX 7FFDC000
004015A7	. 8915 D452D400	MOV DWORD PTR DS:[4052D4],EDX	

Infine inseriamo un nuovo breakpoint all'indirizzo 004015AF, dove troviamo un altro operatore logico, AND. Il valore del registro ECX è 0A280105 (170.393.861 in decimale).

Registers (FPU)

EAX	0A280105
ECX	0A280105
EDX	00000001
EBX	7FFEDC000

Come detto sopra, ci troviamo davanti ad un'operazione AND tra ECX e 0FF, l'esadecimale per 255; l'operatore AND compare i due valori nella loro forma binaria e salva il risultato nel registro ECX, il cui nuovo valore sarà 5.

0A280105 = 1010001010000000000100000101

**0FF** ≡ 11111111

004015AD	. 8BC8	MOV ECX,EAX	EAX 0A280105
004015AF	. 81E1 FF000000	AND ECX,0FF	ECX 00000005
004015B5	. 890D D0524000	MOV DWORD PTR DS:[4052D0],ECX	EDX 00000001

Il malware usa la funzione WSAStartup (indirizzo 00401265), quindi sicuramente si connette alla rete, crea un socket e ottiene l'indirizzo IP della macchina target.

Guardando le funzioni presenti, sembra che possa anche aprire file dal file system e creare heap sulla RAM.