

# Relazione S11L3

Lo scopo dell'esercizio di oggi consiste nell'effettuare l'analisi dinamica avanzata di un malware attraverso l'utilizzo di OllyDBG.

Vengono richiesti i seguenti punti:

**1. 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)**

00401056	. 52	PUSH EDX	pProcessInfo pStartupInfo CurrentDir = NULL pEnvironment = NULL CreationFlags = 0 InheritHandles = TRUE pThreadSecurity = NULL pProcessSecurity = NULL CommandLine = "cmd" ModuleFileName = NULL
00401057	. 8045 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	CreateProcessA
0040106E	. FF15 04404000	CALL DWORD PTR DS:[<&KERNEL32.CreatePro	

Come possiamo vedere dal programma, il parametro CommandLine ha il valore settato a “cmd”. Ci viene mostrato tra i vari parametri passati alla funzione.

**2. Inserite un breakpointsoftware 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)**

00401577	. 55	PUSH EBP	SE handler installation
00401578	. 8BEC	MOV EBP,ESP	
0040157A	. 6A FF	PUSH -1	
0040157C	. 68 C0404000	PUSH Malware_.004040C0	
00401581	. 68 30204000	PUSH Malware_.0040209C	
00401586	. 64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	. 50	PUSH EAX	
0040158D	. 64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	. 8BEC 10	SUB ESP,10	
00401597	. 53	PUSH EBX	
00401598	. 56	PUSH ESI	
00401599	. 57	PUSH EDI	
0040159A	. 8965 E8	MOV DWORD PTR SS:[EBP-18],ESP	
0040159B	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	
0040159C	. 33D2	XOR EDX,EDX	kernel32.GetVersion
004015A3	. 8004	MOV DL,AH	
004015A7	. 9215 D4524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC8	MOV ECX,EDX	
004015AF	. 81E1 FF000000	AND ECX,0FF	
004015B5	. 9300 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	. C1E1 08	SHL ECX,8	
004015BE	. 0BCA	ADD ECX,EDX	
004015C0	. 9300 CC524000	MOV DWORD PTR DS:[4052CC],ECX	
004015C6	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CE	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 8EC0	TEST EAX,EAX	
004015D8	. 75 08	JNZ SHORT Malware_.004015E2	
004015DA	. 6A 1C	PUSH 1C	
004015DC	. E8 9A000000	CALL Malware_.0040167B	
004015E1	. 59	POP ECX	
004015E2	. 8B65 FC 00	AND DWORD PTR SS:[EBP-4],0	

**Registers (FPU)**  
EAX 0A280105  
ECX 7FFD4000  
EDX 00000000  
EBX 7FFD4000  
ESP 0012F794  
EBP 0012FFC0  
ESI FFFFFFFF  
EDI 7C910208 ntdll.7C910208  
EIP 004015A5 Malware\_.004015A5  
C 0 ES 0023 32bit 0(FFFFFFFF)  
P 1 CS 001B 32bit 0(FFFFFFFF)  
A 0 SS 0023 32bit 0(FFFFFFFF)  
Z 1 DS 0023 32bit 0(FFFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(FFF)  
T 0 GS 0000 NULL  
O 0  
O 0 LastErr ERROR\_INVALID\_HANDLE (00000006)  
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)  
ST0 empty -UNORM BCBC 01050104 005C0030  
ST1 empty +UNORM 0069 006E0069 002E0067  
ST2 empty 0.0  
ST3 empty 0.0  
ST4 empty 0.0  
ST5 empty 0.0  
ST6 empty 0.0  
ST7 empty 0.0  
3 2 1 0 E S P U O Z D I  
FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 (GT)  
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

Il valore del registro EDX è 00000000 questo perché viene effettuato uno XOR EDX, EDX e lo xor tra due valori uguali torna sempre 0. In pratica viene inizializzato il registro EDX.

Il valore di ECX inizialmente è 7FFDF000

00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
0040157A	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:01 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	9965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159D	CF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	3302	XOR EDX,EDX	
004015A5	8A04	MOV DL,AH	
004015A7	8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A9	8B03	MOV ECX,EBX	
004015AB	81E1 FF000000	AND ECX,0FF	
004015B5	890D 05240000	MOV DWORD PTR DS:[4052D0],ECX	
00401577	55	PUSH EBP	
00401578	8BEC	MOV EBP,ESP	
0040157A	6A FF	PUSH -1	
0040157C	68 C0404000	PUSH Malware_.004040C0	
00401581	68 3C204000	PUSH Malware_.0040203C	
00401586	64:01 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	50	PUSH EAX	
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP	
00401594	8BEC 10	SUB ESP,10	
00401597	53	PUSH EBX	
00401598	56	PUSH ESI	
00401599	57	PUSH EDI	
0040159A	9965 E8	MOV DWORD PTR SS:[EBP-10],ESP	
0040159D	CF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	3302	XOR EDX,EDX	
004015A5	8A04	MOV DL,AH	
004015A7	8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015A9	8B03	MOV ECX,EBX	
004015AB	81E1 FF000000	AND ECX,0FF	

Al secondo breakpoint invece possiamo vedere che è 0A280105. Quello che vediamo dalle righe del codice assembly è che viene copiato il valore di EAX su ECX e poi viene fatto un AND tra ECX e 0FF e se è vero il valore di ECX viene modificato.

#### 4. BONUS: spiegare a grandi linee il funzionamento del malware

Guardando su VirusTotal e sempre con OllyDBG si capisce che questo è malware è molto probabilmente un trojan che modifica e crea i processi del sistema operativo.

Davide Lecci