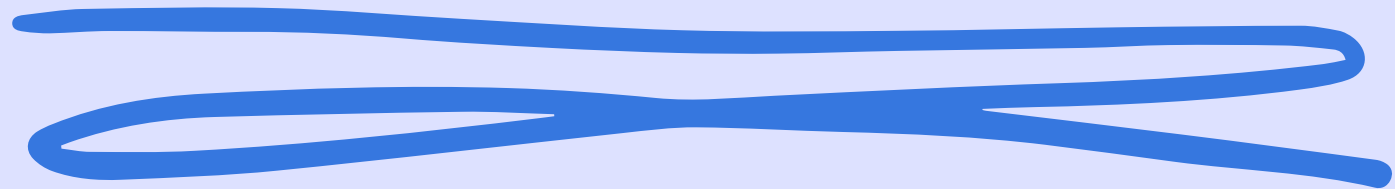


# S11 L3

## Analisi Dinamica Avanzata



**Daniele Zizzi**

## 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**? **(1)**
- 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 **(4)**. Che istruzione è stata eseguita? **(5)**
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? **(6)**  
Eseguite un step-into. Qual è ora il valore di ECX? **(7)** Spiegate quale istruzione è stata eseguita **(8)**.
- BONUS: spiegare a grandi linee il funzionamento del malware

Effettua una chiamata alla dll Kernel32 e crea un processo. Come parametro in CommandLine, gli passa "cmd".

Ipotizzo che, le seguenti righe di codice, aprono un prompt dei comandi.

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.CreatePro	CreateProcessA

Il valore del registro di EDX è A28.

Dopo l'operazione logica XOR tra EDX ed EDX, quindi se stesso, il risultato è 0. Poichè XOR(exclusive OR), viene usato per pulire/impostare a 0 un registro.

La XOR da come risultato 1(vero), solo se gli ingressi sono diversi tra di loro. Se entrambi gli ingressi hanno lo stesso valore, l'uscita sarà 0 (falso).

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:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	50	PUSH EAX	
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00401594	83EC 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	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	890D 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	
004015BE	03CA	ADD ECX,EDX	
004015C0	890D 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	

Registers (FPU)  
EAX 0A280105  
ECX 7FFDA000  
EDX 00000A28  
EBX 7FFDA000  
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)  
A 0 SS 0023 32bit 0(FFFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(FFF)  
T 0 GS 0000 NULL  
D 0  
O 0 LastErr ERROR\_INVALID\_HANDLE (00000006)  
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)  
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

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:A1 00000000	MOV EAX,DWORD PTR FS:[0]	
0040158C	50	PUSH EAX	
0040158D	64:8925 00000000	MOV DWORD PTR FS:[0],ESP	
00401594	83EC 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	
0040159D	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	33D2	XOR EDX,EDX	
004015A5	8AD4	MOV DL,AH	
004015A7	8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	8BC8	MOV ECX,EAX	
004015AF	81E1 FF000000	AND ECX,0FF	
004015B5	890D 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015B8	C1E1 08	SHL ECX,8	
004015BE	03CA	ADD ECX,EDX	
004015C0	890D 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	

Registers (FPU)  
EAX 0A280105  
ECX 7FFDB000  
EDX 00000000  
EBX 7FFDB000  
ESP 0012FF94  
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  
D 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

Il valore corrente di ECX è 280105  
che diventa 5 dopo l'operazione logica AND  
tra ECX e il valore esadecimale 0FF.

280105=0010100000000000100000101

0FF=0000000000000000000011111111

5=0000000000000000000000000000101

La porta logica AND, restituisce 1 quando  
entrambi gli ingressi sono a 1, diversamente,  
restituisce 0.

```
00401577 55 PUSH EBP
00401578 8BEC MOV EBP,ESP
0040157A 6AFF PUSH -1
0040157C 68C0404000 PUSH Malware_.004040C0
00401581 683C204000 PUSH Malware_.0040203C
00401586 64A1000000 MOV EAX,DWORD PTR FS:[0]
0040158C 50 PUSH EAX
0040158D 6489250000 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 8965E8 MOV DWORD PTR SS:[EBP-18],ESP
0040159D FF1530404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion]
004015A3 33D2 XOR EDX,EDX
004015A5 8A04 MOV DL,AH
004015A7 8915D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD 8BC8 MOV ECX,EAX
004015B0 81E1FF000000 AND ECX,0FF
004015B5 8900D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015B8 C1E108 SHL ECX,8
004015BE 03CA ADD ECX,EDX
004015C0 8900CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 C1E810 SHR EAX,10
004015C9 A3C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE 6A00 PUSH 0
004015D0 E833090000 CALL Malware_.00401F08
004015D5 59 POP ECX
```

Registers (FPU)

EAX 0A280105  
ECX 0A280105  
EDX 00000001  
EBX 7FFDA000  
ESP 0012FF94  
EBP 0012FFC0  
ESI FFFFFFFF  
EDI 7C910208 ntdll.7C910208  
EIP 004015AF Malware\_.004015AF

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  
D 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

```
00401577 55 PUSH EBP
00401578 8BEC MOV EBP,ESP
0040157A 6AFF PUSH -1
0040157C 68C0404000 PUSH Malware_.004040C0
00401581 683C204000 PUSH Malware_.0040203C
00401586 64A1000000 MOV EAX,DWORD PTR FS:[0]
0040158C 50 PUSH EAX
0040158D 6489250000 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 8965E8 MOV DWORD PTR SS:[EBP-18],ESP
0040159D FF1530404000 CALL DWORD PTR DS:[<&KERNEL32.GetVersion]
004015A3 33D2 XOR EDX,EDX
004015A5 8A04 MOV DL,AH
004015A7 8915D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015AD 8BC8 MOV ECX,EAX
004015B0 81E1FF000000 AND ECX,0FF
004015B5 8900D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015B8 C1E108 SHL ECX,8
004015BE 03CA ADD ECX,EDX
004015C0 8900CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 C1E810 SHR EAX,10
004015C9 A3C8524000 MOV DWORD PTR DS:[4052C8],EAX
004015CE 6A00 PUSH 0
004015D0 E833090000 CALL Malware_.00401F08
004015D5 59 POP ECX
```

Registers (FPU)

EAX 0A280105  
ECX 00000005  
EDX 00000001  
EBX 7FFDA000  
ESP 0012FF94  
EBP 0012FFC0  
ESI FFFFFFFF  
EDI 7C910208 ntdll.7C910208  
EIP 004015B5 Malware\_.004015B5

C 0 ES 0023 32bit 0(FFFFFFFF)  
P 1 CS 001B 32bit 0(FFFFFFFF)  
A 0 SS 0023 32bit 0(FFFFFFFF)  
Z 0 DS 0023 32bit 0(FFFFFFFF)  
S 0 FS 003B 32bit 7FFDF000(FFF)  
T 0 GS 0000 NULL  
D 0  
O 0 LastErr ERROR\_INVALID\_HANDLE (00000006)  
EFL 00000206 (NO,NB,NE,A,NS,PE,GE,G)  
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

Il malware in questione, apre una linea di comando e richiama la libreria `WS2_32.dll`, che permette di creare un socket, al fine di collegarsi all'esterno della macchina. Si avvia al login in windows.  
Sembrerebbe una backdoor, un attacco di tipo reverse shell.