

A decorative graphic on the left side of the slide, consisting of a network of white lines and small circles on a blue gradient background, resembling a circuit board or a neural network.

ES LEZIONE 3 SETTIMANA 11

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

1°

OllyDbg - Malware_U3_W3_L3.exe - [CPU - main thread, module Malware_]

File View Debug Plugins Options Window Help

Assembly window showing instructions:

```

0040104A . 8945 E8 MOV DWORD PTR SS:[EBP-18],EAX
0040104D . 8B4D E8 MOV ECX,DWORD PTR SS:[EBP-18]
00401050 . 894D E4 MOV DWORD PTR SS:[EBP-1C],ECX
00401053 . 8D55 F0 LEA EDX,DWORD PTR SS:[EBP-10]
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
0040106C . 6A 00 PUSH 0
0040106E . FF15 04404000 CALL DWORD PTR DS:[<&KERNEL32.CreatePro
00401074 . 8945 EC MOV DWORD PTR SS:[EBP-14],EAX
00401077 . 6A FF PUSH -1
00401079 . 8B4D F0 MOV ECX,DWORD PTR SS:[EBP-10]
0040107C . 51 PUSH ECX
0040107D . FF15 00404000 CALL DWORD PTR DS:[<&KERNEL32.WaitForSi
00401083 . 33C0 XOR EAX,EAX
00401085 . 8BE5 MOV ESP,EBP

```

Data window showing structure:

```

pProcessInfo
pStartupInfo
CurrentDir = NULL
pEnvironment = NULL
CreationFlags = 0
InheritHandles = TRUE
pThreadSecurity = NULL
pProcessSecurity = NULL
CommandLine = "cmd"
ModuleFileName = NULL

```

Registers (FPU) window showing:

```

EAX 76A133B8 kernel32.BaseThre
ECX 00000000
EDX 00401577 Malware_.<ModuleEr
EBX 7EFDE000
ESP 0018FF8C
EBP 0018FF94
ESI 00000000
EDI 00000000
EIP 00401577 Malware_.<ModuleEr

```

Address Hex dump ASCII

00405030 00 00 00 00 00 00 00 00

1°

Il valore del parametro "commandLine" che viene passato sullo stack è "Malware_.00405030".

2°3°4°5°

00401573	> FC	CLD			
00401574	. 5F	POP EDI			
00401575	. C9	LEAVE			
00401576	. C3	RETN			
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]	SE handler installation		
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:[4052041],EDX			

00401573	> FC	CLD			
00401574	. 5F	POP EDI			
00401575	. C9	LEAVE			
00401576	. C3	RETN			
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]	SE handler installation		
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:[4052041],EDX			

- 2° Inizialmente il valore di EDX è "00001DB1"
- 3° Successivamente il valore diventa "00000000"
- 4° Questo perché è stata eseguita la funzione dell'indirizzo "4015A3" ossia "XOR EDX,EDX."
- 5° L'OR esclusivo (XOR) è un'operazione tra due bit in cui il bit risultante vale 0 se i due bit comparati sono uguali.

6°7°8°

The top screenshot shows the assembly code at address 004015AF, which is the instruction `AND ECX, 0FF`. The register values on the right show `ECX` as `1DB10106`. The bottom screenshot shows the assembly code at address 004015B5, which is the instruction `SHL ECX, 8`. The register values on the right show `ECX` as `00000006`.

Address	Disassembly	Comment
00401580	<code>MOV DWORD PTR FS:[0],ESP</code>	
00401594	<code>SUB ESP,10</code>	
00401597	<code>PUSH EBX</code>	
00401598	<code>PUSH ESI</code>	
00401599	<code>PUSH EDI</code>	
0040159A	<code>MOV DWORD PTR SS:[EBP-18],ESP</code>	
0040159D	<code>CALL DWORD PTR DS:[<&kernel32.GetVersion]</code>	<code>kernel32.GetVersion</code>
004015A3	<code>XOR EDX,EDX</code>	
004015A5	<code>MOV DL,AH</code>	
004015A7	<code>MOV DWORD PTR DS:[4052D4],EDX</code>	
004015AD	<code>MOV ECX,EAX</code>	
004015AF	<code>AND ECX,0FF</code>	
004015B5	<code>MOV DWORD PTR DS:[4052D0],ECX</code>	
004015B8	<code>SHL ECX,8</code>	
004015BE	<code>ADD ECX,EDX</code>	
004015C0	<code>MOV DWORD PTR DS:[4052CC],ECX</code>	
004015C6	<code>SHR EAX,10</code>	
004015C9	<code>MOV DWORD PTR DS:[4052C8],EAX</code>	
004015CE	<code>PUSH 0</code>	

6° Inizialmente il valore di `ECX` è "1DB10106"

7° Successivamente il valore diventa "00000006"

8° Questo perché è stata eseguita la funzione dell'indirizzo "4015AF" ossia "AND ECX,OFF". Ossia la comparazione logica (AND) tra i due valori.