

# S11/L3

Malware analysis

# 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 **OillyDBG**.

01.

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?

2.1

Inserite un breakpointsoftware all'indirizzo 004015A3. Qual è il valore del registro EDX?

2.2

Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX

2.3

Motivando la risposta, Che istruzione è stata eseguita?

03.

Inserite un secondo breakpointall'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?

3.1

Eseguite un step-into. Qual è ora il valore di ECX?

3.2

Spiegate quale istruzione è stata eseguita

BONUS

Spiegare a grandi linee il funzionamento del malware

# 01. Funzione CreateProcess

All'indirizzo **0440106E**, il malware esegue una chiamata alla funzione **CreateProcess**, come illustrato nella figura seguente.

È importante notare i commenti presenti nella colonna di destra, inseriti automaticamente dal programma **OillyDBG**, che forniscono una breve descrizione del comportamento del malware.

00401053	. 8055 F0	LEA EDX, DWORD PTR SS:[EBP-10]	pProcessInfo
00401056	. 52	PUSH EDX	pStartupInfo
00401057	. 8045 A8	LEA EAX, DWORD PTR SS:[EBP-58]	CurrentDir = NULL
0040105A	. 50	PUSH EAX	pEnvironment = NULL
0040105B	. 6A 00	PUSH 0	CreationFlags = 0
0040105D	. 6A 00	PUSH 0	InheritHandles = TRUE
0040105F	. 6A 00	PUSH 0	pThreadSecurity = NULL
00401061	. 6A 01	PUSH 1	pProcessSecurity = NULL
00401063	. 6A 00	PUSH 0	CommandLine = "cmd"
00401065	. 6A 00	PUSH 0	ModuleFileName = NULL
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	Timeout = INFINITE
00401077	. 6A FF	PUSH -1	
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	hObject
0040107C	. 51	PUSH ECX	WaitForSingleObject
0040107D	. FF15 00404000	CALL DWORD PTR DS:[&KERNEL32.WaitForSi	

Dall'analisi della figura, si osserva che il valore del parametro **CommandLine** è impostato su **cmd**.

# 02. Registro EDX

## 2.1: Qual'è il valore del registro EDX?

Per soddisfare questa richiesta, è stato inizialmente inserito un breakpoint software (**Toggle Breakpoint**) all'indirizzo **004015A3**, dopodiché è stato eseguito il programma.

0040159H	:	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
0040159D	:	FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion] kernel32.GetVersion
<b>004015A3</b>	.	<b>33D2</b>	<b>XOR EDX,EDX</b>
004015A5	:	8AD4	MOV DL,AH
004015A7	:	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX

In questo modo è stato possibile determinare il valore del registro **EDX** richiesto dall'esercizio, pari a **00001DB1**.

<b>004015A3</b>	.	<b>33D2</b>	<b>XOR EDX,EDX</b>
<b>Registers (FPU)</b>			
EAX	<b>10B10106</b>	ECX	<b>7EFDE000</b>
EDX	<b>00001DB1</b>	EBX	<b>7EFDE000</b>
ESP	<b>0018FF5C</b>	EBP	<b>0018FF88</b>
ESI	<b>00000000</b>	EDI	<b>00000000</b>
EIP	<b>004015A3</b>	Malware_.004015A3	

# 02. Registro EDX

2.2-2.3: Eseguite a questo punto uno “step-into”. Indicate qual’è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?

Successivamente, è stato eseguito un **step-into** per esaminare le righe di codice ed entrare nell'implementazione della funzione chiamata.

Controllando nuovamente il registro **EDX**, si nota che il suo valore è cambiato, come illustrato nella figura sottostante.

Tale variazione è dovuta all'esecuzione dell'istruzione logica **XOR**.

Questa operazione restituisce un output pari a 1 quando i due valori di input sono diversi.

Poiché l'operazione **XOR** è stata applicata agli stessi input, ovvero **EDX** e **EDX**, l'output risulterà sempre 0. Di conseguenza, il nuovo valore del registro **EDX** è 0.

Istruzione eseguita: **XOR**.

004015A3	. 3302	XOR EDX, EDX
004015A5	: 8AD4	MOU DL, AH
<b>Registers (FPU)</b>		
EAX	1DB10106	
ECX	7EFDE000	
<b>EDX</b>	<b>00000000</b>	
EBX	7EFDE000	
ESP	0018FF5C	
EBP	0018FF88	
ESI	00000000	
EDI	00000000	
EIP	<b>004015A5</b>	Malware_.004015A5



# 03. Registro ECX

Dopo aver inserito un secondo breakpoint all'indirizzo **004015AF** ed eseguito nuovamente il programma, è stato possibile rilevare il valore del registro **ECX**.

In questa fase dell'analisi, il valore del registro **ECX** risulta essere **1DB10106**.

004015AF	. 81E1 FF000000	AND ECX,0FF
<b>Registers (FPU)</b>		
EAX	1DB10106	
ECX	<b>1DB10106</b>	
EDX	<b>00000001</b>	
EBX	7EFDE000	
ESP	0018FF5C	
EBP	0018FF88	
ESI	00000000	
EDI	00000000	
EIP	<b>004015AF</b>	Malware_.004015AF

# 03. Registro ECX

3.2-3.3: Eseguite un step-into. Qual'è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Successivamente è stato eseguito uno step-into, utilizzato per esaminare righe di codice e a fronte di una chiamata di una funzione accedere alla sua implementazione.

Ricontrollando il registro ECX ora si nota che il suo valore è cambiato, come mostrato in figura sotto.



Registers (FPU)	
EAX	1DB10106
ECX	00000006
EDX	00000001
EBX	7EFDE000
ESP	0018FF5C
EBP	0018FF88
ESI	00000000

Operazione	Hex	Bin
AND	1DB1 0106	0001 1101 1011 0001 0000 0001 0000 0110
	FF	1111 1111
	0000 0006	0000 0000 0000 0000 0000 0000 0000 0110

Il nuovo valore contenuto nel registro **ECX** è il risultato dell'operazione illustrata nella **tabella a fianco**.

# Bonus. Funzionamento del malware

Dopo aver completato questa analisi dinamica, abbiamo utilizzato **CFF Explorer** per confermare le nostre ipotesi.

Dall'analisi, è emerso che il malware apre una **CMD** e che **CFF Explorer** importa le librerie **Kernel32.dll** e **WS2\_32.dll**.

The screenshot shows the CFF Explorer interface with the title bar "CFF Explorer VIII - [Malware\_U3\_W3\_L3.exe]". The menu bar includes "File", "Settings", and "?". Below the menu is a toolbar with icons for file operations. The main area has a tree view on the left and a table view on the right.

**Tree View (Left):**

- File: Malware\_U3\_W3\_L3.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
  - Data Directories [x]
  - Section Headers [x]
  - Import Directory

**Table View (Right):**

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	38	00004460	00000000	00000000	00004562	00004000
WS2_32.dll	7	000044FC	00000000	00000000	0000457E	0000409C

# Bonus. Funzionamento del malware

Per ottenere ulteriori conferme, abbiamo copiato l'**hash** del malware su **VirusTotal**.

Il risultato ha identificato il **malware** come un **trojan**.

Un **trojan** è un tipo di software malevolo che si presenta come un programma legittimo o utile per indurre l'utente a eseguirlo, consentendo così all'attaccante di ottenere accesso non autorizzato al sistema o di eseguire altre attività dannose.

The screenshot shows the VirusTotal analysis interface for a specific file hash. At the top, a large circular progress bar indicates a **Community Score** of **46 / 75**, with a red segment representing vendor detections. A message above the bar states **46/75 security vendors flagged this file as malicious**. Below the bar, the file's SHA-256 hash is listed as **f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133**, and its name is **Malware\_U3\_W3\_L3.exe**. The file is identified as a **peexe** and has tags for **armadillo**, **idle**, and **checks-user-input**. To the right, the file's **Size** is **24.00 KB** and the **Last Analysis Date** is **2 hours ago**. The file is categorized as an **EXE** file. Below the main header, there are tabs for **DETECTION**, **DETAILS**, **RELATIONS**, **BEHAVIOR**, and **COMMUNITY** (with 11 items). A green banner at the bottom encourages users to **Join our Community** for additional insights. At the very bottom, threat labels include **Popular threat label** **trojan.genericrxet/generik**, **Threat categories** **trojan**, and **Family labels** **genericrxet**, **generik**, and **neanvzc**.