

# OillyDBG

**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.

- 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).

1)

00401056	. 52	PUSH EDX	pProcessInfo
00401057	. 8045 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
00401074	. 8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
00401077	. 6A FF	PUSH -1	Timeout = INFINITE
00401079	. 8B4D F0	MOV ECX,DWORD PTR SS:[EBP-10]	
0040107C	. 51	PUSH ECX	hObject
0040107D	. FF15 00404000	CALL DWORD PTR DS:[<&KERNEL32.WaitForSi	WaitForSingleObject
00401083	. 33C0	XOR EAX,EAX	
00401085	. 8BE5	MOV ESP,EBP	
00401087	. 5D	POP EBP	
00401088	. C3	RETN	

Come possiamo vedere dalla figura il parametro "ComandLine" è "cmd" il che potrebbe indicare l'avvio di una finestra del terminale all'avvio del malware.

2)

00401577	. 5E	PUSH EBP	
00401578	. 8BEC	MOV EBP,ESP	
00401579	. 6A FF	PUSH -1	
0040157C	. 68 00404000	PUSH Malware_.004040C0	
00401581	. 68 3C204000	PUSH Malware_.0040203C	
00401586	. 64A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation
0040158C	. 50	PUSH EAX	
0040158D	. 6418925 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	
0040159D	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
004015A3	. 8AD4	MOV DL,AH	
004015A7	. 8915 04524000	MOV DWORD PTR DS:[4052D4],EDX	
004015AD	. 8BC3	MOV ECX,EBX	
004015B5	. 01E1 FF000000	AND ECX,0FF	
004015B8	. 9960 00524000	MOV DWORD PTR DS:[4052D0],ECX	
004015BB	. C1E1 08	SHL ECX,8	
004015BE	. 03CA	ADD ECX,EDX	
004015C0	. 9960 CC524000	MOV DWORD PTR DS:[4052C0],ECX	
004015C3	. C1E8 10	SHR EAX,10	
004015C9	. A3 C8524000	MOV DWORD PTR DS:[4052C8],EAX	
004015CC	. 6A 00	PUSH 0	
004015D0	. E8 33090000	CALL Malware_.00401F08	
004015D5	. 59	POP ECX	
004015D6	. 85C0	TEST EAX,EAX	
004015E2	. 75 08	JNZ SHORT Malware_.00401F02	

EAX	00200105
ECX	7FF00000
EDX	00000028
EBX	7FF00000
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)
G	0 DS 0023 32bit 0(FFFFFFFF)
S	0 FS 003B 32bit 7FF00001(FFF)
T	0 GS 0000 NULL
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

Possiamo vedere che EDX ha valore 0000A28, ma dopo aver eseguito il malware e fatto lo step-into possiamo vedere come il valore passa a 000000.

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV EBP, ESP	
00401579	PUSH -1	
0040157A	PUSH Malware_.004040C0	
0040157B	PUSH Malware_.0040203C	
0040157C	MOV EDI, DWORD PTR FS:[0]	SE handler installation
0040157D	PUSH EAX	
0040157E	MOV DWORD PTR FS:[0], ESP	
0040157F	SUB ESP, 10	
00401580	PUSH EAX	
00401581	PUSH ESI	
00401582	PUSH EDI	
00401583	MOV DWORD PTR SS:[EBP-18], ESP	
00401584	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
00401585	MOV DL, AH	
00401586	MOV DWORD PTR DS:[4052D4], EDI	
00401587	MOV ECX, EAX	
00401588	AND ECX, 0FF	
00401589	MOV DWORD PTR DS:[4052D0], ECX	
0040158A	SHL ECX, 8	
0040158B	ADD ECX, EDX	
0040158C	MOV DWORD PTR DS:[4052CC], ECX	
0040158D	SHR EAX, 10	
0040158E	MOV DWORD PTR DS:[4052C8], EAX	
0040158F	PUSH 0	
00401590	CALL Malware_.00401F08	
00401591	POP ECX	
00401592	TEST EAX, EAX	
00401593	JNZ SHORT Malware_.004015E2	

Register	Value
EAX	0A280105
ECX	0A280105
EDX	00000000
EBX	77FD4000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208
EIP	004015A5

Questo vuol dire che l'operazione XOR è stata eseguita correttamente, ed il malware a modificato il valore del registro.

4)

Address	Disassembly	Comment
00401577	PUSH EBP	
00401578	MOV EBP, ESP	
00401579	PUSH -1	
0040157A	PUSH Malware_.004040C0	
0040157B	PUSH Malware_.0040203C	
0040157C	MOV EDI, DWORD PTR FS:[0]	SE handler installation
0040157D	PUSH EAX	
0040157E	MOV DWORD PTR FS:[0], ESP	
0040157F	SUB ESP, 10	
00401580	PUSH EAX	
00401581	PUSH ESI	
00401582	PUSH EDI	
00401583	MOV DWORD PTR SS:[EBP-18], ESP	
00401584	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	kernel32.GetVersion
00401585	MOV DL, AH	
00401586	MOV DWORD PTR DS:[4052D4], EDI	
00401587	MOV ECX, EAX	
00401588	AND ECX, 0FF	
00401589	MOV DWORD PTR DS:[4052D0], ECX	
0040158A	SHL ECX, 8	
0040158B	ADD ECX, EDX	
0040158C	MOV DWORD PTR DS:[4052CC], ECX	
0040158D	SHR EAX, 10	
0040158E	MOV DWORD PTR DS:[4052C8], EAX	
0040158F	PUSH 0	
00401590	CALL Malware_.00401F08	
00401591	POP ECX	
00401592	TEST EAX, EAX	
00401593	JNZ SHORT Malware_.004015E2	
00401594	PUSH 1C	
00401595	CALL Malware_.0040167B	
00401596	POP ECX	

Register	Value
EAX	0A280105
ECX	0A280105
EDX	00000000
EBX	77FD4000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C910208
EIP	004015A5

il valore del registro ECX è **0A280105**.

Il valore cambia in quando viene compiuta l'operazione AND con 0FF ( ricordiamo che 0FF in esadecimale equivale a 255). Quindi vengono messi a confronto il registro EAX con il valore 255, bit per bit. Se i bit corrispondono allora il valore è uno se no 0.

## Bonus:

Dopo essere andato a recuperare MD5 Hash del malware da CFF Explore, ed averlo caricato su Virus Total è risultato evidente che fosse un Trojan.

42

/ 68

Community Score

ⓘ 42 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133

Size24.00 KB

Last Analysis Date23 days ago

peexe

idle

armadillo

checks-user-input

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY10

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ

Do you want to automate checks?

Alibaba	ⓘ Trojan:Win32/Generic.5a8eecd3	ALYac	ⓘ Application.Agent.AHB
Antiy-AVL	ⓘ Trojan/Win32.BTSGeneric	Arcabit	ⓘ Application.Agent.AHB
Avast	ⓘ Win32:Malware-gen	AVG	ⓘ Win32:Malware-gen
BitDefender	ⓘ Application.Agent.AHB	BitDefenderTheta	ⓘ Gen:NN.ZexaF.36680.bmW@aaPI0K
Bkav Pro	ⓘ W32.Common.D47F939F	CrowdStrike Falcon	ⓘ Win/malicious_confidence_100% (W)
Cybereason	ⓘ Malicious.eb3fbd	Cylance	ⓘ Unsafe

CFF Explorer VIII - [Malware\_U3\_W3\_L3.exe]

File Settings ?

File: Malware\_U3\_W3\_L3.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Address Converter

Dependency Walker

Hex Editor

Identifier

Import Adder

Quick Disassembler

Rebuilder

Resource Editor

UPX Utility

Malware\_U3\_W3\_L3.exe

Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	24.00 KB (24576 bytes)
PE Size	24.00 KB (24576 bytes)
Created	Tuesday 16 August 2022, 13.37.31
Modified	Saturday 30 April 2011, 17.24.22
Accessed	Wednesday 14 February 2024, 14.32.29
MD5	251F4D0CAF6EADAE453488F9C9C0EA95
SHA-1	EA8E109EB3FBDB76623CF9522267345B19721E42

Property	Value
Empty	No additional info available