

CS0124

REPORT

PROGETTO

S11L3

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).

**a questa riga di comando possiamo vedere il valore
cmd assegnato.**

Seconda consegna

dopo aver avviato il processo e aggiunto il breakpoint software alla riga indicata
vediamo che edx assume il valore 00000000 e il processo viene reinizializzato grazie
al comando XOR



0040155F	. F7D9	NEG ECX		ECX 7EFDE000
00401561	. 4F	DEC EDI		EDX 00000000
00401562	. 8A45 0C	MOV AL, BYTE PTR SS:[EBP+C]		EBX 7EFDE000
00401565	. FD	STD		ESP 0018FF5C
00401566	. F2:AE	REPNE SCAS BYTE PTR ES:[EDI]		EBP 0018FF88
00401568	. 47	INC EDI		ESI 00000000
00401569	. 3807	CMP BYTE PTR DS:[EDI], AL		EDI 00000000
0040156B	✓ 74 04	JE SHORT Malware_.00401571		EIP 004015A5 Malware_.004015A5
0040156D	. 33C0	XOR EAX, EAX		C 0 ES 002B 32bit 0(FFFFFFFF)
0040156F	✓ EB 02	JMP SHORT Malware_.00401573		P 1 CS 002B 32bit 0(FFFFFFFF)
00401571	> 8BC7	MOV EAX, EDI		A 0 SS 002B 32bit 0(FFFFFFFF)
00401573	> FC	CLD		Z 1 DS 002B 32bit 0(FFFFFFFF)
00401574	. 5F	POP EDI		S 0 FS 0053 32bit 7EFDD000(FFF)
00401575	. C9	LEAVE		T 0 GS 002B 32bit 0(FFFFFFFF)
00401576	. C3	RETN		D 0
00401577 <ModuleEntryPoint>	55	PUSH EBP		O 0 LastErr ERROR_SUCCESS (00000000)
00401578	. 8BEC	MOV EBP, ESP		EFL 00000246 (NO, NB, E, BE, NS, PE, GE, LE)
0040157A	. 6A FF	PUSH -1		ST0 empty 0.0
0040157C	. 68 C0404000	PUSH Malware_.004040C0	SE handler installation	ST1 empty 0.0
00401581	. 68 3C204000	PUSH Malware_.0040203C		ST2 empty 0.0
00401586	. 64:A1 00000000	MOV EAX, DWORD PTR FS:[0]		ST3 empty 0.0
0040158C	. 50	PUSH EAX		ST4 empty 0.0
0040158D	. 64:8925 00000000	MOV DWORD PTR FS:[0], ESP		ST5 empty 0.0
00401594	. 83EC 10	SUB ESP, 10		ST6 empty 0.0
00401597	. 53	PUSH EBX		ST7 empty 0.0
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		

3 2 1 0 E S P U O Z
 FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0
 FCW 027F Prec NEAR, 53 Mask 1 1 1 1

Terza consegna

Il valore iniziale di ecx di 1DB10106, successivamente il valore cambia e diventa 00000006 poiche' la riga di codice copia il valore di eax in ecx e successivamente esegue un AND tra ecx e 0FF

Quarta consegna

Osservando il codice attraverso virus total vediamo che il malware sembra essere un trojan

The screenshot shows the VirusTotal analysis interface for a file named `Malware_U3_W3_L3.exe`. The file's SHA-256 hash is `f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133`. The file size is 24.00 KB, and it was last analyzed 13 days ago. A circular progress indicator shows a score of 44 out of 71, with a red warning icon indicating that 44 security vendors and no sandboxes flagged the file as malicious. The file is categorized as a trojan, specifically `trojan.genericrxet/meanvzc`. The analysis also shows several behavioral tags: `peexe`, `idle`, `armadillo`, and `checks-user-input`. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (with 10 members). A banner at the bottom encourages joining the VT Community for additional insights and API access.

44 / 71

44 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

f153dfacec09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133

Size 24.00 KB Last Analysis Date 13 days ago

Malware_U3_W3_L3.exe

peexe idle armadillo checks-user-input

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 10

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

Popular threat label `trojan.genericrxet/meanvzc` Threat categories trojan Family labels genericrxet

GRAZIE!