



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)

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.CreateProcessA]	CreateProcessA
00401074	• 8B45 EC	MOV EAX, DWORD PTR SS:[EBP-14]	

Dall'analisi del codice, notiamo che il parametro CommandLine è assegnato al valore "cmd" all'interno del programma. Questa informazione è evidenziata tra i diversi argomenti trasmessi alla funzione.

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)**

Il registro EDX contiene attualmente il valore 00000000, poiché è eseguita un'operazione XOR tra EDX e se stesso ($EDX \oplus EDX$), il che restituisce sempre 0. Di conseguenza, il registro EDX viene inizializzato a zero.

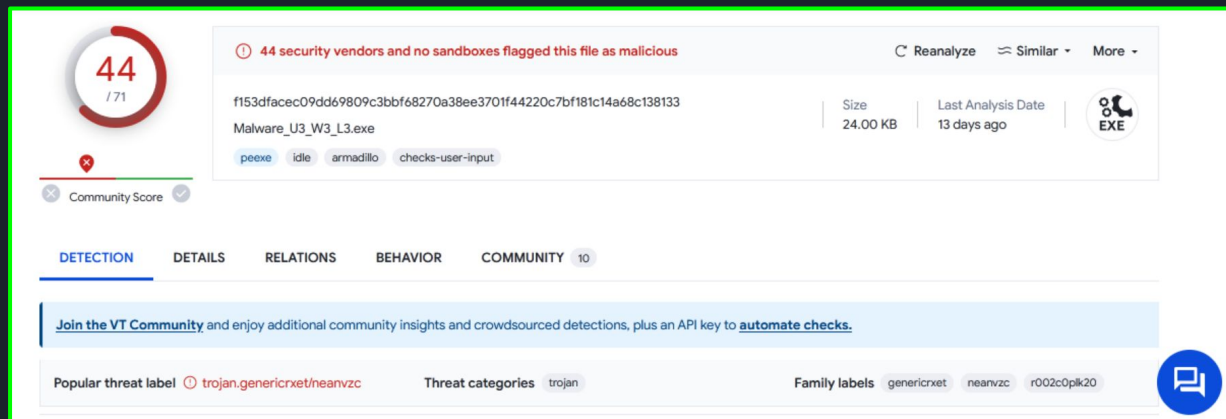
Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6)
Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).

Address	Disassembly	Comment	Registers (FPU)
00401577	55	PUSH EBP	EAX: 0A280105
00401578	8BEC	MOV EBP, ESP	ECX: 7FFDF000
00401579	6A FF	PUSH -1	EDX: 00000001
0040157C	68 C0404000	PUSH Malware_.004040C0	EBX: 7FFDF000
00401581	68 3C204000	PUSH Malware_.0040203C	ESP: 0012FF94
00401586	64:R1 00000000	MOV EAX, DWORD PTR FS:[0]	EBP: 0012FFC0
0040159C	50	PUSH EAX	ESI: FFFFFFFF
0040158D	64:8925 000000	MOV DWORD PTR FS:[0], ESP	EDI: 7C910208 ntdll.7C910208
00401594	8BEC 10	SUB ESP, 10	EIP: 004015A0 Malware_.004015A0
00401597	53	PUSH EBX	C 0 ES: 0023 32bit 0(FFFFFFFF)
00401598	56	PUSH ESI	P 1 CS: 001B 32bit 0(FFFFFFFF)
00401599	57	PUSH EDI	A 0 SS: 0023 32bit 0(FFFFFFFF)
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18], ESP	Z 1 DS: 0023 32bit 0(FFFFFFFF)
0040159B	FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion	S 0 FS: 0038 32bit 7FFDE000(FFF)
0040159C	3302	XOR EDX, EDX	T 0 GS: 0000 NULL
0040159D	8AD4	MOV DL, AH	D 0
004015A5	9915 D4524000	MOV DWORD PTR DS:[4052D4], EDX	O 0 LastErr: ERROR_INVALID_HANDLE
004015A7	8BC8	MOV ECX, EAX	
004015A9	81E1 FF000000	AND ECX, 0FF	
004015AB	8960 D0524000	MOV DWORD PTR DS:[4052D0], ECX	

Il valore di ECX iniziale è 7FFDF000

Al secondo breakpoint, notiamo che il valore è 0A280105. Dalle istruzioni nel codice assembly, osserviamo che il contenuto di EAX viene trasferito in ECX e successivamente viene eseguita un'operazione AND tra ECX e 0FF. Se l'operazione restituisce un risultato vero, il valore di ECX viene modificato.

BONUS: spiegare a grandi linee il funzionamento del malware



The screenshot displays the VirusTotal analysis interface for a file named 'Malware_U3_W3_L3.exe'. At the top left, a circular badge shows a score of 44 out of 71. A red warning icon and text state: '44 security vendors and no sandboxes flagged this file as malicious'. The file's SHA-256 hash is 'f153dfac09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133'. Metadata includes a size of 24.00 KB and a last analysis date of 13 days ago. The file icon is labeled 'EXE'. Detection engines listed include 'peexe', 'idle', 'armadillo', and 'checks-user-input'. A 'Community Score' section is partially visible. The navigation bar includes 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' (with a count of 10). A blue banner encourages joining the VT Community. At the bottom, the 'Popular threat label' is 'trojan.genericxet/eanvzc', 'Threat categories' is 'trojan', and 'Family labels' are 'genericxet', 'eanvzc', and 'r002c0pk20'. A blue icon with a document symbol is in the bottom right corner.

44 / 71

44 security vendors and no sandboxes flagged this file as malicious

Reanalyze Similar More

f153dfac09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133

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.genericxet/eanvzc

Threat categories: trojan

Family labels: genericxet eanvzc r002c0pk20

Caricando il file su VirusTotal ci viene “detto” che si tratta molto probabilmente di un trojan.