

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

Tramite l'utilizzo del tool OllyDBG siamo riusciti a rispondere ai seguenti quesiti:

- 1) All'indirizzo 0040106E il valore del parametro Command Line è impostato su CMD come visibile in figura

00401040	. 8B40 EB	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.CreateProcessA>]	CreateProcessA
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.WaitForSingleObject>]	WaitForSingleObject
00401083	. 33C0	XOR EAX, EAX	
00401085	. 8BE5	MOV ESP, EBP	

- 2) Dopo aver inserito un Breakpoint all'indirizzo indicato, possiamo constatare che il valore del registro EDX è 00000A28

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	. 64:01 00000000	MOV EAX, DWORD PTR FS:[0]	
0040158C	. 50	PUSH EAX	
0040158D	. 64:8925 00000000	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	
0040159B	. FF15 30404000	CALL DWORD PTR DS:[<&KERNEL32.GetVersion>]	kernel32.GetVersion
004015A3	. 33D2	XOR EDX, EDX	
004015A5	. 8D04	MOV DL, AH	
004015A7	. 8915 D4524000	MOV DWORD PTR DS:[405204], EDX	
004015AB	. 8B03	MOV ECX, EAX	
004015AF	. 81E1 FF000000	AND ECX, 0FF	
004015B5	. 8900 D0524000	MOV DWORD PTR DS:[405200], ECX	
004015B8	. C1E1 08	SHL ECX, 8	

Registers (FPU)	
EAX	0A280105
ECX	7FFD9000
EDX	00000A28
EBX	7FFD9000
ESP	0012FF94
EBP	0012FFC0
ESI	FFFFFFFF
EDI	7C920208 ntdll.7C920208
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)
Z 0	DS 0023 32bit 0(FFFFFFFF)
S 0	FS 003B 32bit 7FFD9000(FFF)
T 0	GS 0000 NULL
O 0	LastErr ERROR_INVALID_HANDLE (00000006)
EFL	00000206 (NO, NB, NE, A, NS, PE, GE, G)

- 1-4-5) Dopo aver eseguito uno “Step-Into” il valore del registro EDX è 00000000, questo perché viene eseguita l’istruzione XOR EDX,EDX che da come valore 0, perché lo XOR tra due valori uguali da come risultato sempre 0

00401577	55	PUSH EBP			
00401578	8BEC	MOV EBP,ESP			
00401579	6A FF	PUSH -1			
0040157C	68 C0404000	PUSH Malware_.004040C0			
00401581	68 3C204000	PUSH Malware_.0040203C			
00401586	64:R1 00000000	MOV EAX,DWORD PTR FS:[0]			
0040158C	50	PUSH EAX			
0040158D	64:8925 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		
004015A5	33D2	XOR EDX,EDX			
004015A5	8AD4	MOV DL,AH			
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX			
004015A8	8BC3	MOV ECX,EDX			
004015AF	81E1 FF000000	AND ECX,0FF			
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX			
004015B8	C1E1 08	SHL ECX,8			

Registers (FPU)
 EAX 0A280105
 ECX 0A280105
 EDX 00000000
 EBX 7FFD9000
 ESP 0012FF94
 EBP 0012FFC0
 ESI FFFFFFFF
 EDI 7C920208 ntdll.7C920208
 EIP 004015A5 Malware_.004015A5
 C 0 ES 0023 32bit 0(FFFFFFFF)
 P 1 CS 001B 32bit 0(FFFFFFFF)
 A 0 SS 0023 32bit 0(FFFFFFFF)
 Z 1 DS 0023 32bit 0(FFFFFFFF)
 S 0 FS 0038 32bit 7FFDF000(FFF)
 T 0 GS 0000 NULL
 D 0
 O 0 LastErr ERROR_INVALID_HANDLE (00000006)
 EFL 00010246 (NO,NB,E,BE,HS,PE,GE,LE)

- 6-7-8) Dopo aver inserito un Breakpoint all’indirizzo indicato il valore del registro ECX è 0A280105 e dopo aver eseguito uno “Step-Into” il valore è 00000005, perché è stata eseguita l’istruzione AND ECX,0FF che corrisponde all’esadecimale indicato.

00401577	55	PUSH EBP			
00401578	8BEC	MOV EBP,ESP			
00401579	6A FF	PUSH -1			
0040157C	68 C0404000	PUSH Malware_.004040C0			
00401581	68 3C204000	PUSH Malware_.0040203C			
00401586	64:R1 00000000	MOV EAX,DWORD PTR FS:[0]			
0040158C	50	PUSH EAX			
0040158D	64:8925 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		
004015A5	33D2	XOR EDX,EDX			
004015A5	8AD4	MOV DL,AH			
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX			
004015A8	8BC3	MOV ECX,EDX			
004015AF	81E1 FF000000	AND ECX,0FF			
004015B5	8900 D0524000	MOV DWORD PTR DS:[4052D0],ECX			
004015B8	C1E1 08	SHL ECX,8			

Registers (FPU)
 EAX 0A280105
 ECX 0A280105
 EDX 00000001
 EBX 7FFD9000
 ESP 0012FF94
 EBP 0012FFC0
 ESI FFFFFFFF
 EDI 7C920208 ntdll.7C920208
 EIP 004015AF Malware_.004015AF
 C 0 ES 0023 32bit 0(FFFFFFFF)
 P 1 CS 001B 32bit 0(FFFFFFFF)
 A 0 SS 0023 32bit 0(FFFFFFFF)
 Z 1 DS 0023 32bit 0(FFFFFFFF)
 S 0 FS 0038 32bit 7FFDF000(FFF)
 T 0 GS 0000 NULL
 D 0
 O 0 LastErr ERROR_INVALID_HANDLE (00000006)
 EFL 00010246 (NO,NB,E,BE,HS,PE,GE,LE)

BONUS) Tramite l’analisi del codice notiamo la presenza delle funzioni Socket e con l’utilizzo di VirtusTotal possiamo dedurre che si tratti di un Trojan che inserisce una backdoor nel sistema infettato

44

7/2

44 security vendors and no sandboxes flagged this file as malicious

f153dfacc09dd69809c3bb6f68270a38ee370f144220c7b181c14a68c138133

Size 24.00 KB

Last Analysis Date 1 hour ago

EXE

peexe ide armadillo checks-user-input

Community Score

DTECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

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

Popular threat label Trojan:generic.exe!nearvzc Threat categories trojan Family labels generic.exe!nearvzc!00320p320

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.36608.bmW@aP0K
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.cb3fd