

ANALISI DINAMICA AVANZATA

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.

- (1) 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) Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX?
- (3) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX
- (4) motivando la risposta
- (5). Che istruzione è stata eseguita?
- (6) Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
- (7) Eseguite un step-into. Qual è ora il valore di ECX?
- (8) Spiegate quale istruzione è stata eseguita.
- (9) Che istruzione è stata eseguita?
- (10) BONUS: Capire di che malware si tratta

All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Aprendo il registro abbiamo visto il valore cmd «CommandLine» viene passato sullo stack

```
pProcessInfo
{
  pStartupInfo
  CurrentDir = NULL
  pEnvironment = NULL
  CreationFlags = 0
  InheritHandles = TRUE
  pThreadSecurity = NULL
  pProcessSecurity = NULL
  CommandLine = "cmd"
  ModuleFileName = NULL
  CreateProcessA
```

Cmd= command line

Dopo aver ricercato l'indirizzo richiesto (004015A3) clicchiamo per eseguire un breakpoint e spostandoci sui registri vediamo il valore del registro EDX.

Registers (FPU)	
EAX	00000000
ECX	0012FFB0
EDX	7C91E4F4 ntdll.KiFastSystemCallRet
EBX	7FFD4000
ESP	0012FFC4
EBP	0012FFF0
ESI	FFFFFFFF
EDI	7C920208 ntdll.7C920208
EIP	00401577 Malware_.<ModuleEntryPoint>

EDX=7C91E4F4

Abbiamo ora eseguito uno step-into e visto che il valore di EDX è stato modificato.

7C81126A	64:A1 18000000	MOV EAX,DWORD PTR FS:[18]	Registers (FPU)
7C811270	8B48 30	MOV ECX,DWORD PTR DS:[EAX+30]	EAX 00000002
7C811273	8B81 B0000000	MOV EAX,DWORD PTR DS:[ECX+B0]	ECX 7FFDF000
7C811279	0FB791 AC000000	MOVZX EDX,WORD PTR DS:[ECX+AC]	EDX 00000A28
7C811280	83F0 FE	XOR EAX,FFFFFFFF	EBX 7FFDF000
7C811283	C1E0 0E	SHL EAX,0E	ESP 0012FF90
7C811286	0BC2	OR EAX,EDX	EBP 0012FFC0
7C811288	C1E0 08	SHL EAX,8	ESI FFFFFFFF
7C81128B	0B81 A8000000	OR EAX,DWORD PTR DS:[ECX+A8]	EDI 7C920208 ntdll.7C920208

Il MOVZX copia il valore da un registro con dimensioni più piccole(8-16 bit) a uno di dimensioni superiori (16-32 bit).

Questo perché il comando MOVZX (nell'istruzione che vediamo nell'immagine) copia il valore di word dentro il registro EDX,

Proprio in quella riga di codice si vede infatti che il valore è stato modificato

Inserendo un secondo breakpoint all'indirizzo di memoria 004015AF. E spostandoci dalla parte dei registri vediamo il valore di ECX

00401593	33D2	XOR EDX,EDX	Registers (FPU)
004015A5	8AD4	MOV DL,AH	EAX 0A280105
004015A7	8915 04524000	MOV DWORD PTR DS:[405204],EDX	ECX 0A280105
004015AD	8BC8	MOV ECX,EAX	EDX 00000001
004015AF	81E1 FF000000	AND ECX,0FF	EBX 7FFDF000
004015B5	890D 00524000	MOV DWORD PTR DS:[4052D0],ECX	ESP 0012FF94
004015B8	C1E1 08	SHL ECX,8	EBP 0012FFC0
004015BE	03CA	ADD ECX,EDX	ESI FFFFFFFF
004015C0	890D CC524000	MOV DWORD PTR DS:[4052CC],ECX	EDI 7C920208 ntdll.7C920208
004015C6	C1E8 10	SHR EAX,10	

Eseguite un step-into notiamo che il valore di ECX cambia appena arriviamo all'istruzione AND ECX, 0FF

Notiamo che il valore verrà cambiato quando sarà eseguita l'istruzione AND con il registro ECX e il valore del numero esadecimale 0FF. il risultato ottenuto è il seguente

```
Registers (FPU)
EAX 0A280105
ECX 00000005
EDX 00000001
EBX 7FFDB000
ESP 0012FF94
EBP 0012FFC0
ESI FFFFFFFF
EDI 7C910208 ntdll.7C910208
EIP 004015B5 Malware_.004015B5
```

Infine è stato analizzato il malware utilizzando il tool cff explorer per ricavarci l'hash in formato md5 che abbiamo riportato su virus total e abbiamo avuto la seguente risposta alla scansione fatta dell'hash

43
/ 72

Community Score

43 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

f153dfac09dd69809c3bbf68270a38ee3701f44220c7bf181c14a68c138133

Size24.00 KB

Last Analysis Date27 days ago

EXE

Lab 6.exe

peexeidlearmadillochecks-user-input

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY10

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

Popular threat labeltrojan.genericxet/nearest

Threat categoriestrojan

Family labelsgenericxetnearestr002c0plk20

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.36792.bmW@aaPI0K
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

Abbiamo dedotto quindi tramite virus total che il malware è un trojan