

EPICODE-CS0124

S11/L3 - Pratica

Flaviano Sedici

Indice

1. Traccia	3
1.1. Chiamata indirizzo 0040106E	4
1.2. Breakpoint software 004015A3	4
1.3. Breakpoint software 004015A3 Step-Into	5
1.4. Breakpoint software 004015A3 Step-Into - dettaglio	5
1.4.1.004015A3 -> XOR EDX, EDX -> EDX = 0	5
1.4.2.004015A5 -> MOV DL, AH -> EDX = 1	6
1.5. Breakpoint software 004015AF	6
1.6. Breakpoint software 004015AF Step-Into	7
1.7. Comportamento del malware	8

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	03/04/2024

1. 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

1.1. Chiamata indirizzo 0040106E

Alla riga indicata il malware effettua una chiamata alla funzione dedicata alla creazione dei processi tramite la libreria KERNEL32.dll. Alla funzione viene passato il parametro alla riga 00401067 commandLine = "cmd" che invoca il prompt dei comandi di Windows.

00401056	52	PUSH EDX	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

Funzione chiamata durante l'esecuzione del malware

1.2. Breakpoint software 004015A3

Inserendo un breakpoint software all'indirizzo indicato dalla traccia, identifichiamo il valore iniziale di EDX come 00001DB1.

CPU - main thread, module Malware_				Registers (FPU)	
00401561	4F	DEC EDI		EAX	10B10106
00401562	8A45 0C	MOV AL,BYTE PTR SS:[EBP+C]		ECX	7EFDE000
00401565	F0	STD		EDX	00001DB1
00401566	F2:AE	REPNE SCAS BYTE PTR ES:[EDI]		EBX	7EFDE000
00401568	47	INC EDI		ESP	0018FF5C
00401569	3B07	CMP BYTE PTR DS:[EDI],AL		EBP	0018FF88
0040156B	74 04	JE SHORT Malware_.00401571		ESI	00000000
0040156D	33C0	XOR EAX,EAX		EDI	00000000
0040156F	EB 02	JMP SHORT Malware_.00401573		EIP	004015A3 Mal
00401571	8BC7	MOV EAX,EDI		C 0	ES 002B 32b
00401573	FC	CLD		P 1	CS 0023 32b
00401574	5F	POP EDI		A 0	SS 002B 32b
00401575	C9	LEAVE		Z 0	DS 002B 32b
00401576	C3	RETN		S 0	FS 0053 32b
00401577	55	PUSH EBP		T 0	GS 002B 32b
00401578	8BEC	MOV EBP,ESP		D 0	
0040157A	6A FF	PUSH -1		O 0	LastErr ERR
0040157C	68 C0404000	PUSH Malware_.004040C0		EFL	00000206 (NO
00401581	68 3C204000	PUSH Malware_.0040203C		ST0	empty 0.0
00401586	64:A1 00000000	MOV EAX,DWORD PTR FS:[0]	SE handler installation	ST1	empty 0.0
0040158C	50	PUSH EAX		ST2	empty 0.0
0040158D	64:8925 000000	MOV DWORD PTR FS:[0],ESP		ST3	empty 0.0
00401594	8BEC 10	SUB ESP,10		ST4	empty 0.0
00401597	53	PUSH EBX		ST5	empty 0.0
00401598	56	PUSH ESI		ST6	empty 0.0
00401599	57	PUSH EDI		ST7	empty 0.0
0040159A	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP		FST	0000 Cond 0
0040159D	FF15 30404000	CALL DWORD PTR DS:[&KERNEL32.GetVersion]	kernel32.GetVersion	FCW	027F Prec N
004015A3	33D2	XOR EDX,EDX			
004015A5	8AD4	MOV DL,AH			
004015A7	8915 D4524000	MOV DWORD PTR DS:[4052D4],EDX			
004015A9	8BC8	MOV ECX,EAX			
004015AB	81E1 FF000000	AND ECX,0FF			
004015B5	890D D0524000	MOV DWORD PTR DS:[4052D0],ECX			

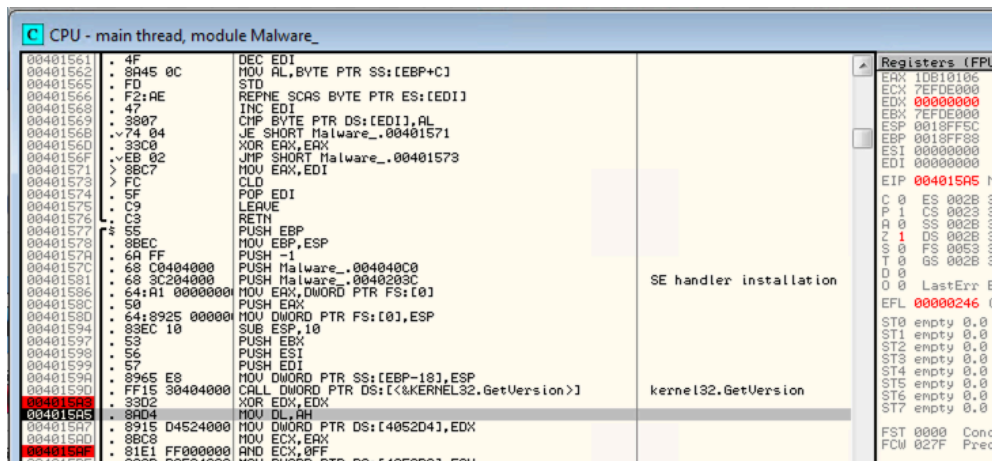
Breakpoint software 004015A3

1.3. Breakpoint software 004015A3 Step-Into

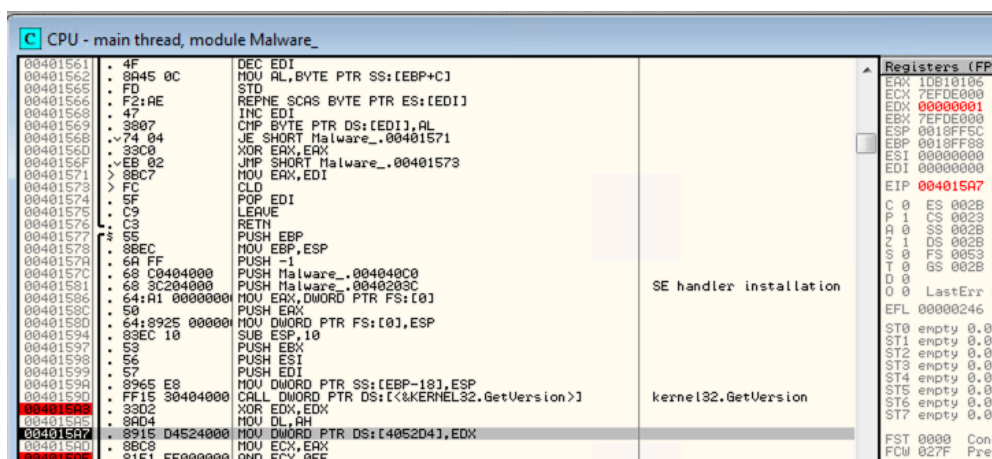
Utilizzando la funzionalità “step-into” possiamo notare che il valore di EDX cambia in questa sequenza:

004015A3 -> EDX = 0

004015A5 -> EDX = 1



Breakpoint software 004015A3+1



Breakpoint software 004015A3+2

1.4. Breakpoint software 004015A3 Step-Into - dettaglio

Passiamo ad analizzare il dettaglio dei due comandi che modificano il valore di EDX.

1.4.1. 004015A3 -> XOR EDX, EDX -> EDX = 0

Il comando **XOR** (Exclusive OR) è un’operazione logica binaria che è stata utilizzata al posto del comando MOV per impostare il valore di **EDX a 0** massimizzando l’efficienza dell’operazione.

Nel caso specifico l’operatore XOR deposita il valore risultante dalla comparazione della sorgente e della destinazione, nella destinazione.

Nel caso specifico, essendo EDX == EDX, imposta il valore di EDX a 0 in quanto l’operatore XOR restituisce Falso o 0 quando i due operandi sono uguali, sia che essi siano Veri o 1, sia che essi siano Falsi o 0.

Essendo la sequenza di bit dei due valori identica, ogni confronto restituirà 0 e quindi il risultato finale sarà paro a 0.

7601 = EDX = 0001 1101 1011 0001

7601 = EDX = 0001 1101 1011 0001

0000 = EDX = 0000 0000 0000 0000

1.4.2. 004015A5 -> MOV DL, AH -> EDX = 1

Il comando riportato alla riga è **MOV DL, AH**. Nel caso specifico DL è una sezione di 8 bit del registro EDX.

Possiamo scomporre il registro **EDX (32 bit)** in **DX (16bit)** che a sua volta viene scomposto in **DL (8bit)** e **DH (8bit)** che vengono utilizzati per memorizzare dati di minore entità per cui sarebbe necessari un numero inferiore di bit.

Nel caso specifico il valore AH (8bit del registro EAX) viene spostato in DL. Essendo presenti in EDX tutti bit a 0, lo stesso registro assume il valore della sua sottosezione, ovvero DL.

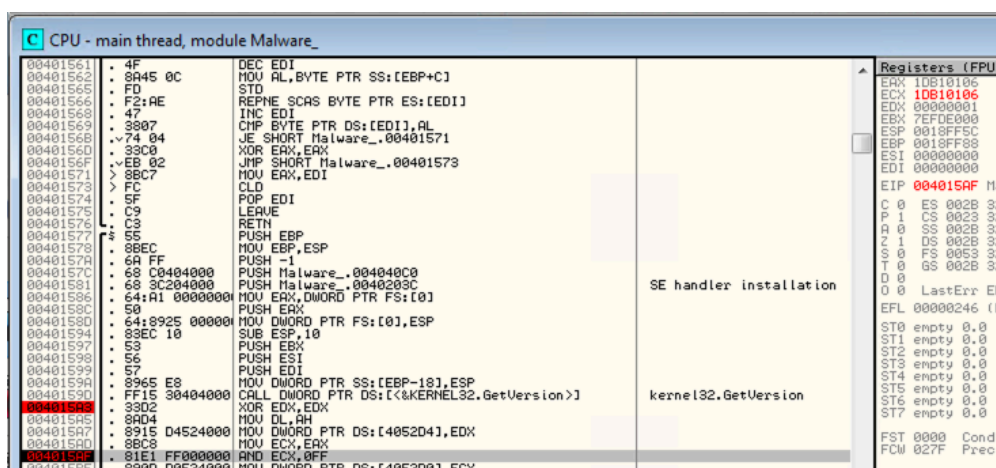
EAX = 1DB10106 = 0001 1101 1011 0001 **0000 0001** 0000 0110

Il valore di AH è composto dal secondo ottetto di EAX e quindi sarà pari a:

AH = **0000 0001** = 1

Quindi il valore di DL sarà pari a AH = 1.

1.5. Breakpoint software 004015AF



Breakpoint software 004015AF

Al breakpoint indicato il valore di **ECX** è pari a **1DB10106**.

1.6. Breakpoint software 004015AF Step-Into

Alla riga di breakpoint viene eseguito il comando **AND ECX, 0FF**.

Il comando **AND** è un'operazione logica binaria che deposita il valore risultante dalla comparazione della sorgente e della destinazione, nella destinazione.

```

CPU - main thread, module Malware_
00401561 . 4F      DEC EDI
00401562 . 8A45 0C  MOV AL, BYTE PTR SS:[EBP+C]
00401565 . FD      STD
00401566 . F2:RE   REPNE SCAS BYTE PTR ES:[EDI]
00401568 . 47      INC EDI
00401569 . 3B07    CMP BYTE PTR DS:[EDI],AL
0040156B . 74 04    JE SHORT Malware_.00401571
0040156D . 33C0    XOR EAX,EAX
0040156F . EB 02    JMP SHORT Malware_.00401573
00401571 . 8BC7    MOV EAX,EDI
00401573 . CD      CWD
00401574 . 5F      POP EDI
00401575 . C9      LEAVE
00401576 . C3      RETN
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:A1 00000000 MOV EAX,DWORD PTR FS:[0]
0040158C . 50      PUSH EAX
0040158D . 64:8925 000000 MOV DWORD PTR FS:[0],ESP
00401594 . 83EC 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>]
004015A3 . 33D2    XOR EDX,EDX
004015A5 . 8A04    MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015A8 . 8BC8    MOV ECX,EAX
004015AB . 81E1 FF000000 AND ECX,0FF
004015B5 . 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX

```

Breakpoint software 004015AF

```

CPU - main thread, module Malware_
00401573 . FC      CLD
00401574 . 5F      POP EDI
00401575 . C9      LEAVE
00401576 . C3      RETN
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:A1 00000000 MOV EAX,DWORD PTR FS:[0]
0040158C . 50      PUSH EAX
0040158D . 64:8925 000000 MOV DWORD PTR FS:[0],ESP
00401594 . 83EC 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>]
004015A3 . 33D2    XOR EDX,EDX
004015A5 . 8A04    MOV DL,AH
004015A7 . 8915 D4524000 MOV DWORD PTR DS:[4052D4],EDX
004015A8 . 8BC8    MOV ECX,EAX
004015AB . 81E1 FF000000 AND ECX,0FF
004015B5 . 8900 D0524000 MOV DWORD PTR DS:[4052D0],ECX
004015B6 . C1E1 08  SHL ECX,8
004015B8 . 03CA    ADD ECX,EDX
004015C0 . 8900 CC524000 MOV DWORD PTR DS:[4052CC],ECX
004015C6 . C1E8 10  SHR EAX,10
004015C9 . A3 C0524000 MOV DWORD PTR DS:[4052C0],EAX
004015CE . 6A 00    PUSH 0
004015D0 . E8 33090000 CALL Malware_.00401F08
004015D5 . 59      POP ECX
004015D6 . 85C0    TEST EAX,EAX

```

Breakpoint software 004015AF+1

In particolare nel confronto bit per bit nel caso i due bit siano uguali il valore risultante è pari ai due valori uguali, altrimenti in caso di disuguaglianza restituisce 0 o Falso.

Nel caso in esame abbiamo:

ECX = 1DB10106 = 0001 1101 1011 0001 0000 0001 0000 0110

AND = 000000FF = 0000 0000 0000 0000 0000 0000 1111 1111

ECX = 00000006 = 0000 0000 0000 0000 0000 0000 0000 0110

1.7. Comportamento del malware

Module Name	Imports
szAnsi	(nFunctions)
KERNEL32.dll	38
WS2_32.dll	7

Librerie importate

Analizzando la tipologia di librerie importate notiamo immediatamente la libreria WS2_32.dll che viene normalmente utilizzata per la gestione del network e la creazione di socket. Possiamo ipotizzare che sia un DNS Changer in quanto importa solo la funzione dedicata alla creazione di socket e funzioni dedicate alla gestione e alla modifica dei thread e dei processi tramite la libreria KERNEL32.dll

L'analisi condotta tramite Virus Totale lo identifica genericamente come Trojan con capacità di modifica e gestione dei DNS, creazione canali HTTPS e TCP client. Ne desumiamo che potrebbe anche essere in grado di scaricare ulteriori pacchetti malevoli su richiesta.

Riferimento [Virus Total](#)