

Progetto S11L5

Traccia 1: Spiegate, motivando, quale salto condizionale effettua il Malware.

CODICE:

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

1.

Viene assegnato 10 a EBX.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

2.

EBX viene incrementato (quindi EBX=11).

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

3.

Se il registro EBX è uguale a 11 (come in questo caso), viene effettuato il salto all'indirizzo 0040FFA0.

Traccia 2: Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.

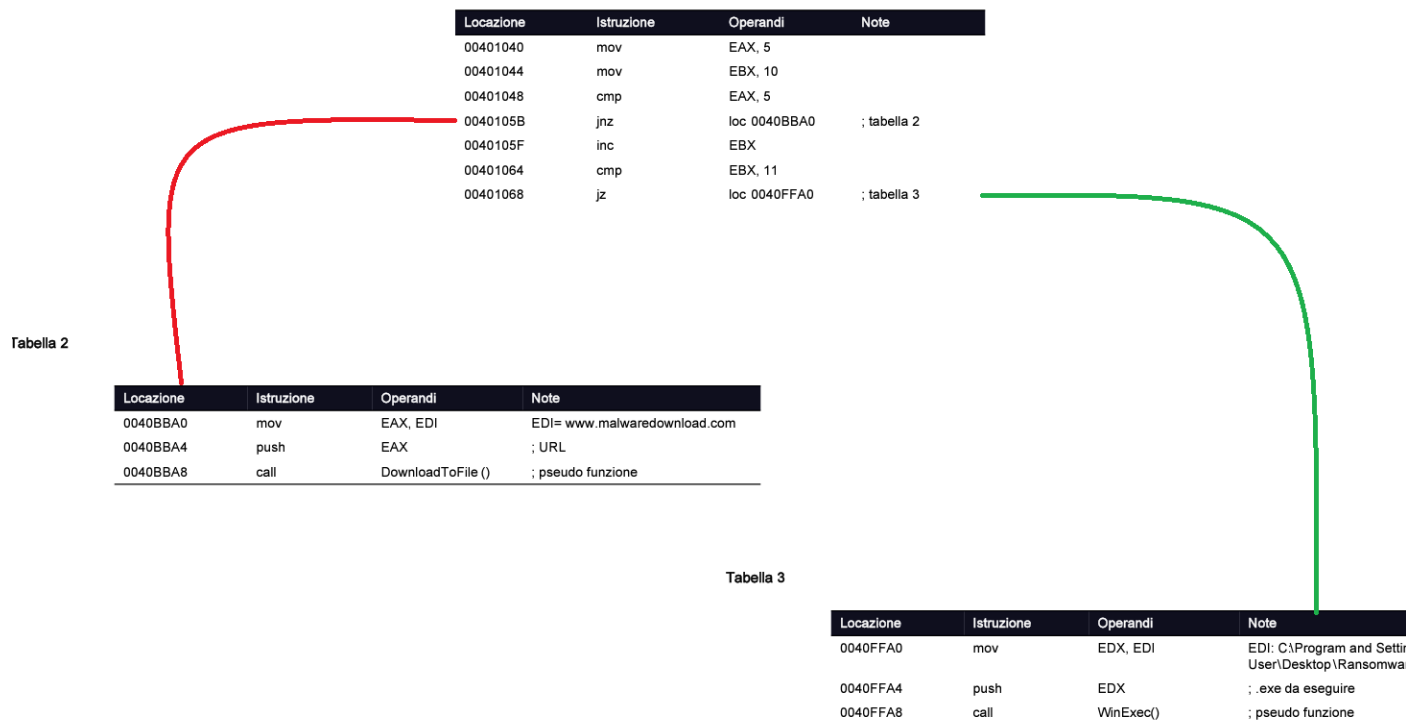
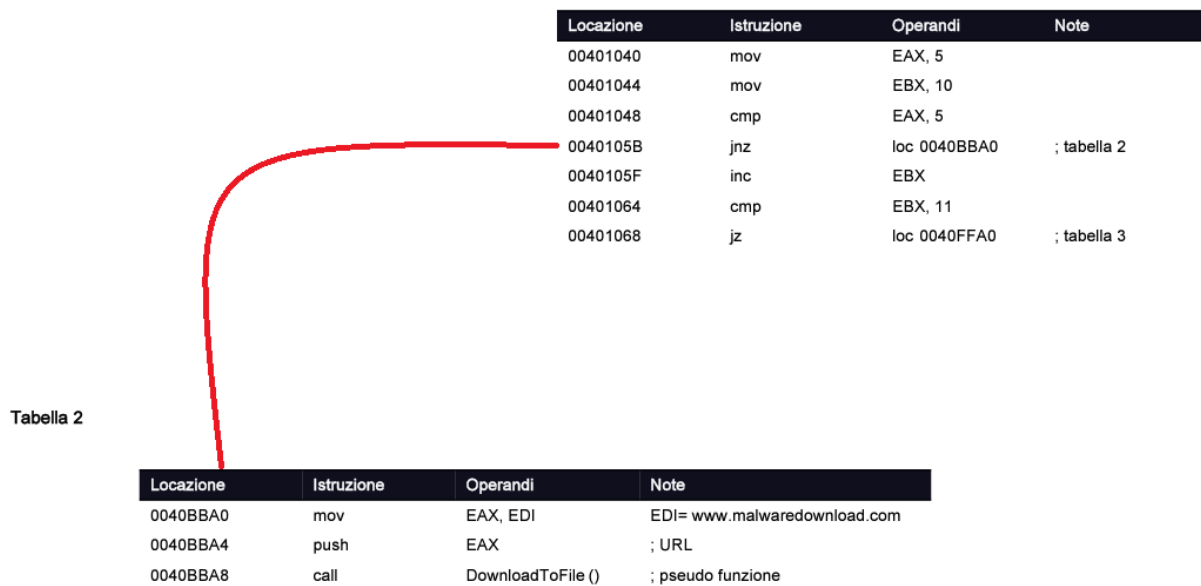


Diagramma di flusso principale.



Qui il salto non viene effettuato in quanto EAX è uguale a 5
(JNZ=se due valori non sono uguali).

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings \Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Qui invece il salto viene effettuato, perché EBX è uguale a 11 e quindi si procede con il salto all'indirizzo 0040FFA0(JZ=se due valori sono uguali).

Traccia 3:Quali sono le diverse funzionalità implementate all'interno del Malware?

- 1)il malware imposta il registro EAX con l'indirizzo "www.malwaredownload.com"(URL da cui scaricare un file dannoso).
- 2)chiama la funzione DownloadToFile(), la quale scarica il file dall'url precedente sul sistema bersaglio.
- 3)il malware imposta il registro EDX con il percorso del file scaricato, "C:\Program and Settings\Local

User\Desktop\Ransomware.exe". Quindi, chiama la funzione WinExec(), la quale esegue il file scaricato.

Il malware è un DOWNLOADER

Traccia 4: Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

Tabella 2

Nella tabella 2, l'istruzione *mov EAX, EDI* imposta il registro EAX con l'indirizzo dell'URL "www.malwaredownload.com" (memorizzato nel registro EDI).

Successivamente il valore di EAX che contiene l'indirizzo dell'URL, viene inserito nello stack con l'istruzione *push EAX*.

Dopodiché, viene effettuata una chiamata alla funzione DownloadToFile(), passando l'URL come argomento.

Tabella 3

Nella tabella 3, l'istruzione *mov EDX, EDI* imposta il registro EDX con il percorso del file "C:\Program and Settings\Local User\Desktop\Ransomware.exe" memorizzato nel registro EDI. Successivamente, il percorso del file viene inserito nello stack con l'istruzione push EDX, e poi viene chiamata la funzione WinExec() che prenderà come argomento Ransomware.exe.

