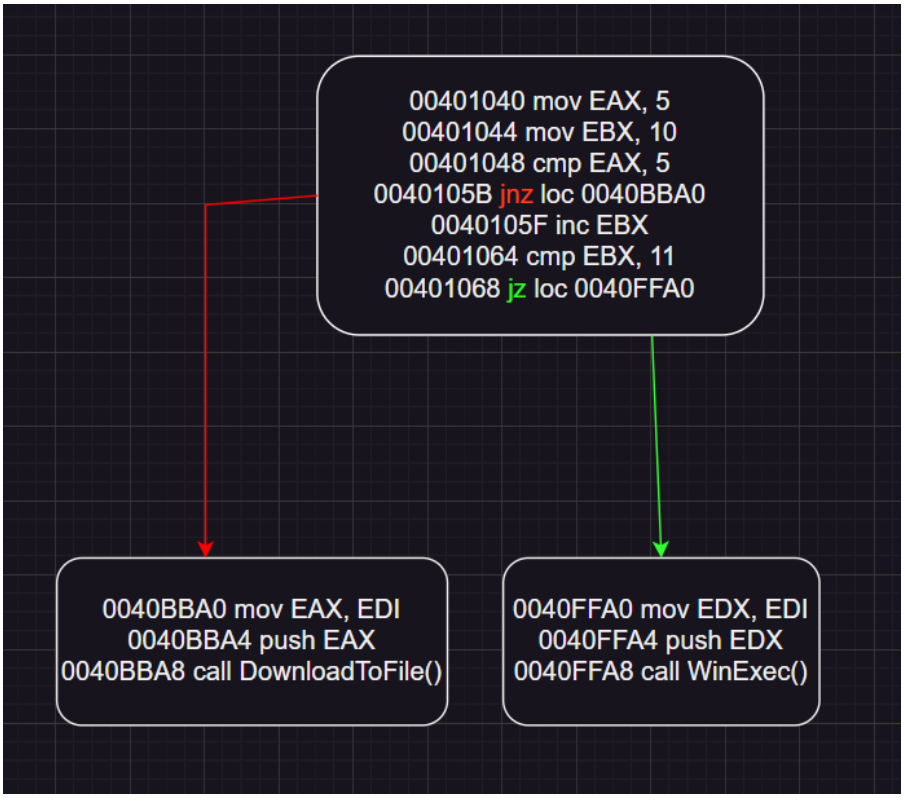
Progetto analisi avanzata

Ernesto Robles

Analizzando il codice raffigurato nella tabella qua presente, si nota come il Malware effettua un salto alla locazione di memoria 00401068, poichè l'istruzione "jz" effettua il salto alla locazione che li viene specificata solo se gli operandi dell'istruzione "cmp" sono uguali e qua possiamo vedere come EBX è pari a 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

Il salto condizionale che viene eseguito è colorato di verde così come la sua istruzione, il salto che non viene eseguito è colorato di rosso.



Delle due funzionalità implementate nel Malware ne verrà eseguita solo una.

La funzionalità che non viene eseguita ovvero quella del salto in rosso evidenzia come il Malware scarichi qualcosa da Internet assumendo così il comportamento da Downloader, mentre la funzionalità che viene eseguita evidenzia come il Malware esegua un altro Malware già presente sul PC locale che probabilmente è stato precedentemente scaricato utilizzando la funzione WinExec().

L'URL (www.malwaredownload.com) viene passato alla funzione DownloadToFile() per lo scaricamento di ulteriori file malevoli, mentre il path dell'eseguibile da avviare viene passato alla funzione WinExec(). I parametri vengono passati sullo stack utilizzando l'istruzione push per entrambe le funzioni DownloadToFile() e WinExec().