Progetto S11_L4

1) Il malware esegue un salto condizionale all'indirizzo di memoria 00401068. Utilizzando l'istruzione “jz”, passa all'indirizzo specificato solo se gli operandi dell'istruzione “cmp” precedente sono uguali, come nel caso in cui EBX è pari a 11. Nel caso in cui, invece, gli operandi dell’istruzione “cmp” precedente non sono uguali (EAX = 5), il malware non attua il salto condizionale.

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) A sinistra (jz) il salto condizionale effettuato, a destra (jnz) quello non effettuato

3) Il malware funziona in due modi in base alla situazione. Può scaricare un altro malware da Internet, agendo da downloader, oppure eseguirne uno presente sulla macchina tramite la funzione “WinExec()”.

4) In riferimento alle istruzioni “call”, sia per la funzione “DownloadToFile()” che per “WinExec()”, i parametri vengono passati allo stack attraverso l’utilizzo di “push”.
La prima funzione riceve l'URL dal quale scaricare il file malevolo, mentre la seconda riceve il percorso (path) dell'eseguibile da avviare. La “call function” corretta per il download del file malevolo da un URL è “URLDownloadToFile()” e non “DownloadToFile()”.