PROGETTO S11-L5

INDICE:

1. TRACCIA:

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

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

PROGETTO S11-L5

2. QUESITO 1

Spiegate, motivando, quale salto condizionale effettua il Malware.

Il Malware in questione sembra effettuare due salti condizionali basati sui risultati di confronti tra registri.

Vediamo nel dettaglio:

Il primo salto condizionale avviene alla locazione **00401048**, dove viene eseguito un confronto tra il contenuto del registro **EAX** e il valore 5 utilizzando l'istruzione **cmp**. Successivamente, viene utilizzata l'istruzione **jnz**, che salta all'indirizzo **0040BBA0** se il risultato del confronto non è uguale a zero (cioè se **EAX** non è uguale a 5). Questo potrebbe essere un tentativo del malware di gestire un caso specifico, probabilmente dipendente dal valore di **EAX**.

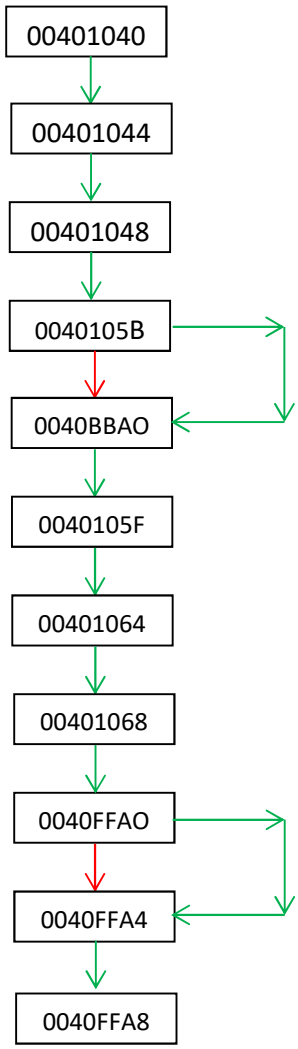
Il secondo salto condizionale si verifica alla locazione **00401068**, dove viene eseguito un confronto tra il contenuto del registro **EBX** e il valore 11. Se il confronto produce un risultato uguale a zero (cioè se **EBX** è uguale a 11), il salto condizionale (**jz**) porterà l'esecuzione alla locazione **0040FFA0**.

In sintesi, il primo salto condizionale sembra essere legato al valore del registro **EAX**, mentre il secondo è legato al valore del registro **EBX**.

PROGETTO S11-L5

3. QUESITO 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.



PROGETTO S11-L5

4. QUESITO 3

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

Sembra che il Malware abbia tre funzionalità principali:

Download di file da un URL malevolo:

- La funzione **DownloadToFile()** viene chiamata dopo aver impostato il registro **EAX** con l'URL malevolo (**EDI**).
- Prima viene caricato l'URL (**EDI**) in **EAX** e quindi pushato nello stack.
- La funzione **DownloadToFile()** presumibilmente scarica un file dal web (nell'URL malevolo) e lo salva in un file locale.

Esecuzione di un file .exe malevolo:

- La funzione **WinExec()** viene chiamata dopo aver impostato il registro **EDX** con il percorso del file .exe malevolo (**EDI**).
- Prima viene caricato il percorso del file **.exe** (**EDI**) in **EDX** e quindi pushato nello stack.
- La funzione **WinExec()** presumibilmente esegue il file .exe specificato.

Controllo del flusso tramite confronti e salti condizionati:

- Ci sono confronti (**cmp**) tra i registri **EAX** ed **EBX**.
- Sono presenti istruzioni di salto condizionato (**jnz** e **jz**) che determinano il flusso del programma in base ai risultati dei confronti.
- Questi controlli di flusso possono essere utilizzati per gestire il comportamento del malware in base a determinate condizioni.

Il Malware è progettato per scaricare e eseguire un file eseguibile malevolo da un URL specifico, mentre i controlli di flusso possono essere utilizzati per aggiungere logica extra, come gestire situazioni di errore o variazioni nel comportamento del sistema.

PROGETTO S11-L5

5. QUESITO 4

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

Le istruzioni "**call**" sono utilizzate per chiamare le funzioni **DownloadToFile()** e **WinExec()**.

Analizziamo come vengono passati gli argomenti a queste chiamate di funzione:

Chiamata alla funzione DownloadToFile() (Tabella 2):

- Prima dell'istruzione **call DownloadToFile()**, viene eseguita un'istruzione **push EAX**.
- Questo mette il valore contenuto nel registro EAX (che è stato precedentemente impostato su "EDI") nello stack.
- Quindi, quando **DownloadToFile()** viene chiamata, l'indirizzo della stringa "www.malwaredownload.com" (che era contenuto in EDI) viene passato come argomento alla funzione tramite lo stack.

Chiamata alla funzione WinExec() (Tabella 3):

- Prima dell'istruzione **call WinExec()**, viene eseguita un'istruzione **push EDX**.
- Questo mette il valore contenuto nel registro EDX (che è stato precedentemente impostato su "EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe") nello stack.
- Quindi, quando **WinExec()** viene chiamata, l'indirizzo del percorso del file ".exe" da eseguire (che era contenuto in EDI) viene passato come argomento alla funzione tramite lo stack.