PROGETTO S11 L5

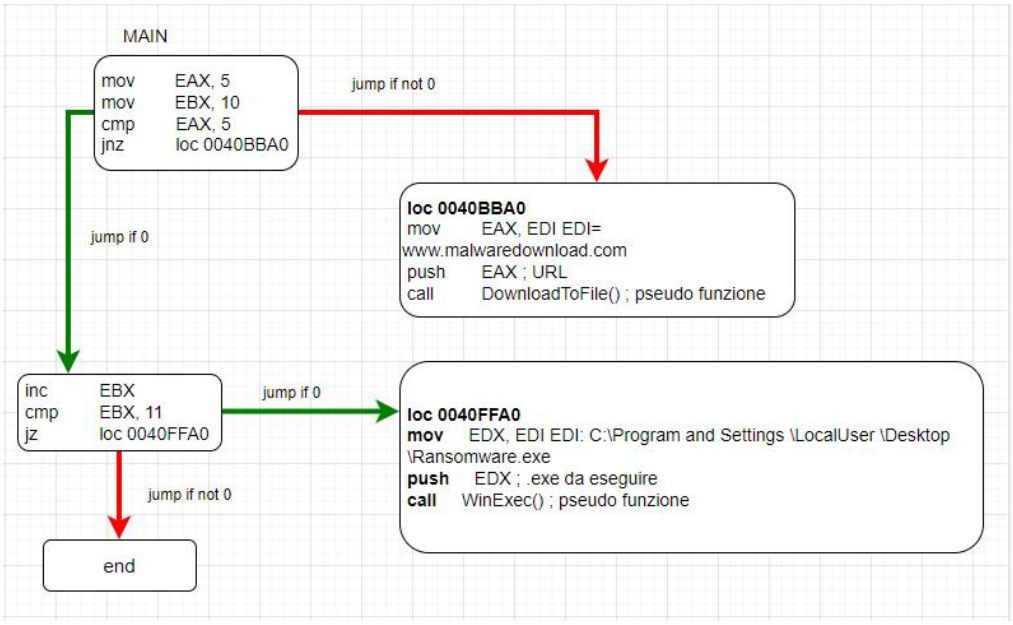
EPICODE

Esercizio
Traccia e requisiti

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.



In questo schema possiamo vedere come il programma salta da un riquadro ad un altro.
Dal quadro MAIN si impostano EAX = 5 e EBX = 10, si compara EAX con 5, e come EAX = 5 allora il FLAG = 0, e jumpa al riquado in basso. In questo riquadro si incrementa EBX +1, e poi si compara EBX con 11, e come ora che incrementato EBX = 11, allora il FLAG = 0 e jumpa a destra compilando le altre righe di codice.
In questa parte di codice EDI viene registrato dentro EDX, dove EDI = C:\Program and Settings \LocalUser \Desktop \Ransomware.exe, quindi il percorso in cui è situato il malware. Puoi EDX viene pushato nello stack de infine viene richiamata la funzione **WinExec**() per permettere si che sia eseguito.

Componenti WinExec()
UINT winexc(
[in] LPCSTR lpcmdline, ---> Questo è un puntatore e rappresenta la riga di comando che verrà passata al programma che si desidera eseguire, contiene il path del file.
[in] UINT ucmdshow ---> permette alla visualizzazione del file, se la finestra viene mostrata o meno.

Il riquado mancante in alto a destra ci indicava come il malware si sarebbe collegato ad un sito dedicato e scaricato in file.

A EAX sarebe stato assegnato l’ URL tramite EDI, e quindi tenta di passare l’ URL alla funzione **DownloadToFile**() per eseguire il download di un file da quel determinato indirizzo, e scarica il file e salvarlo nel disco del computer.

Componenti DownloadToFile()

HRESULT URLDownloadToFile(
LPUNKNOWN pCaller, ----> Un puntatore all'interfaccia IUnknown.
LPCTSTR szURL, ----> Una stringa contenente l'URL del file che si desidera scaricare.
LPCTSTR szFileName, ----> Una stringa contenente il percorso in cui si desidera salvare il file scaricato.
Reserved DWORD dwReserved, ----> Un parametro riservato. Deve essere impostato su zero.
LPBINDSTATUSCALLBACK lpfnCB ----> Un puntatore a una funzione di callback IBindStatusCallback. Questa funzione di callback viene chiamata durante il processo di download per fornire informazioni sullo stato dell'operazione di download.
);