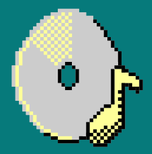
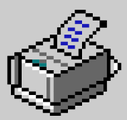


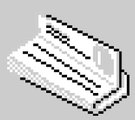




PROGETTO S11/L5

Byterebels.eu





22:10

Traccia:

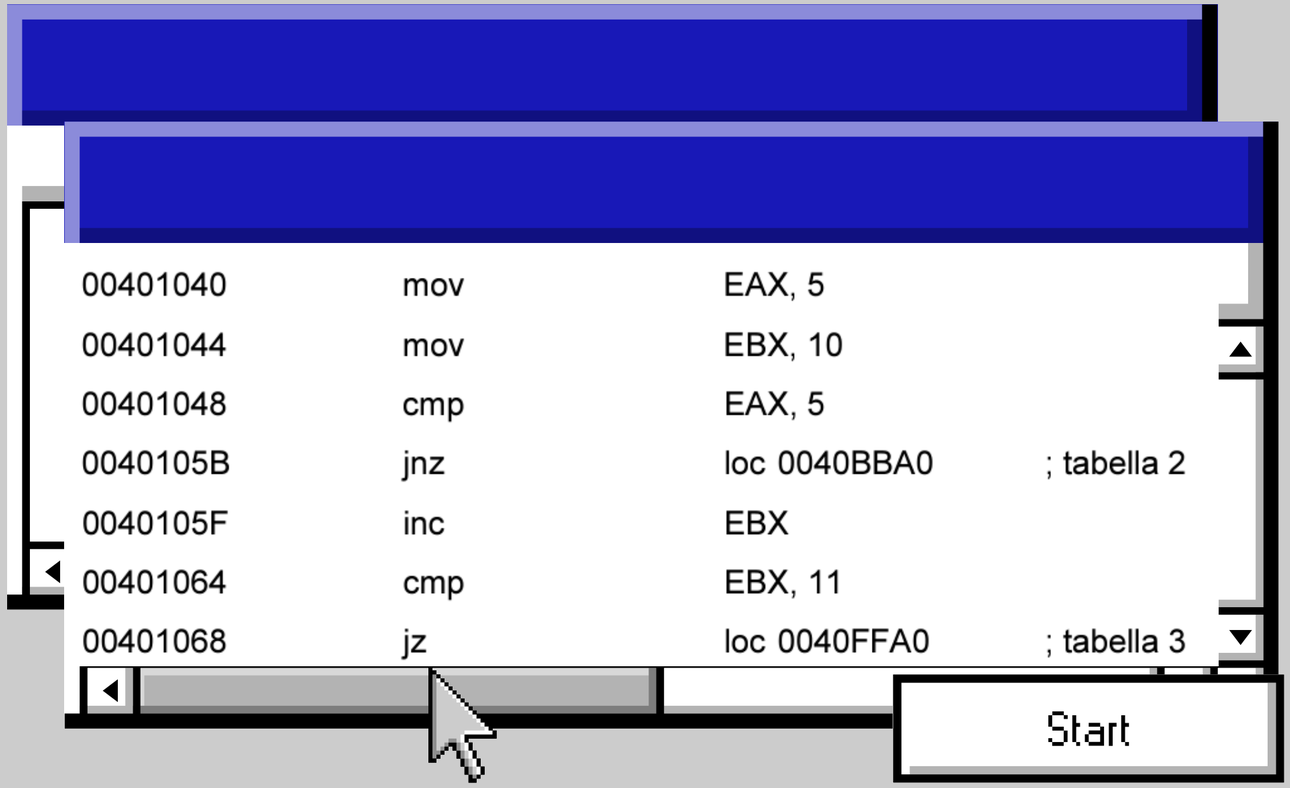
Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

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.

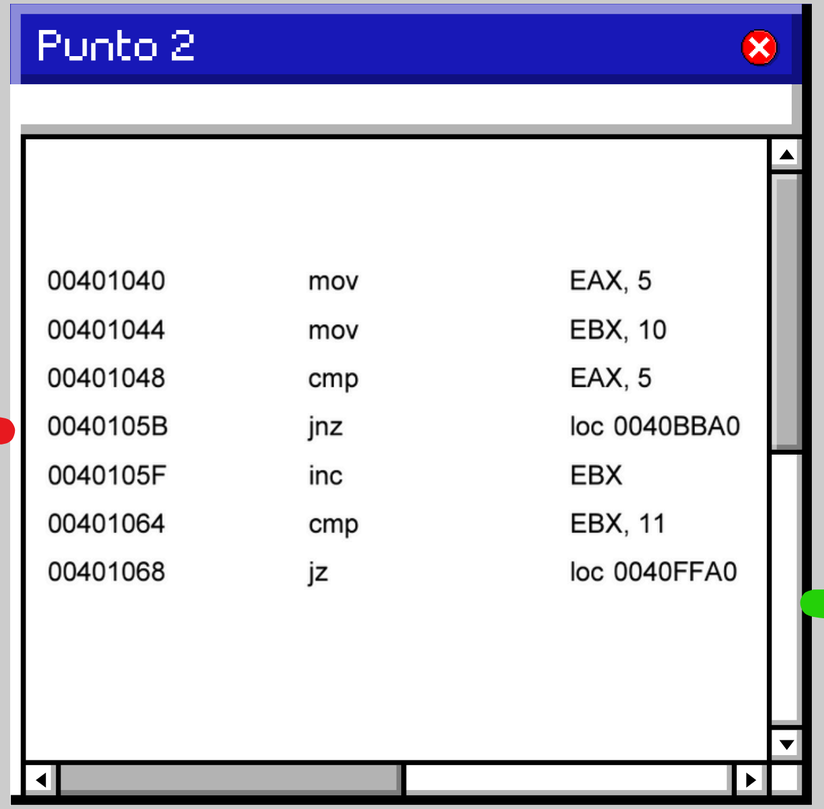
Punto 1

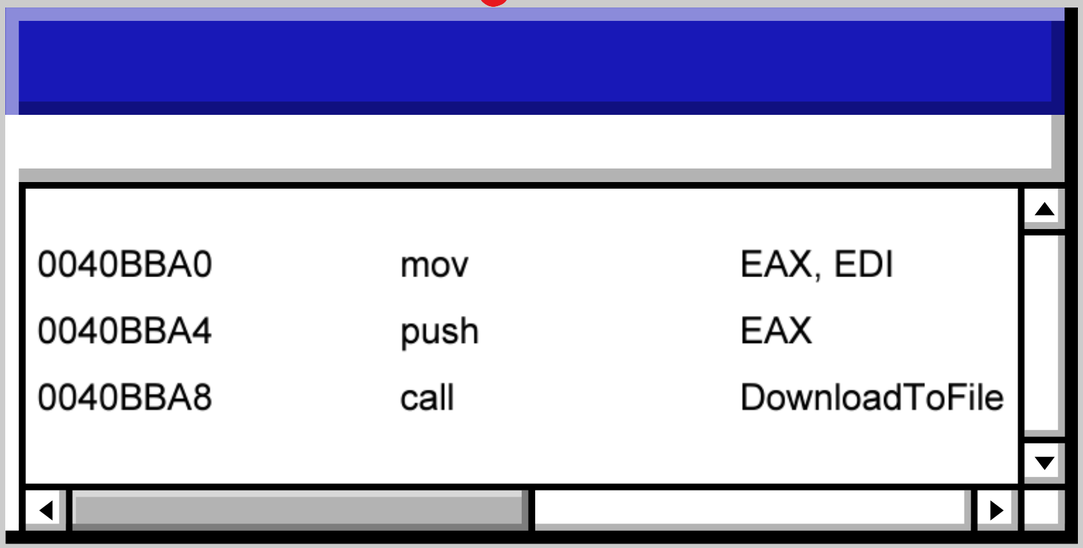
- Spiegate, motivando, quale salto condizionale effettua il Malware

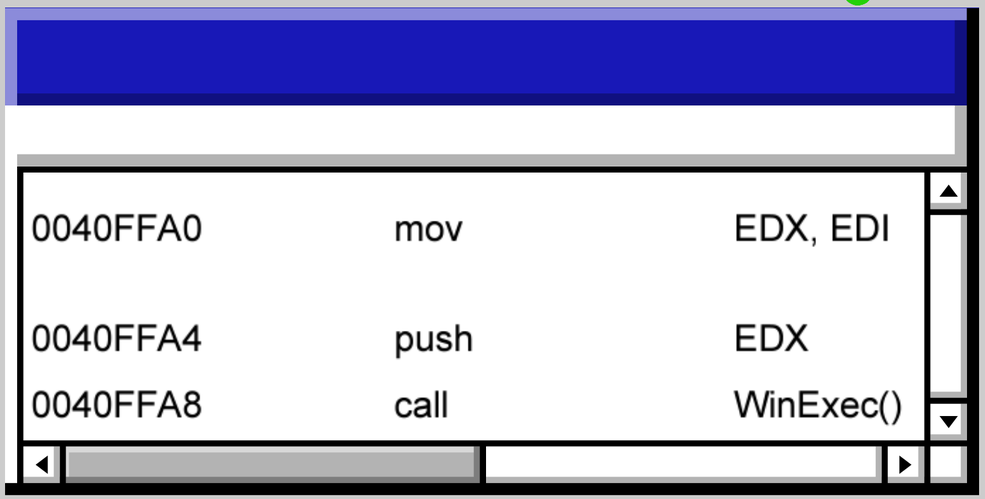
Come notiamo dalla tabella 1, il Malware effettua il salto condizionale presente alla locazione di memoria 00401068.
Infatti, l'istruzione jz esegue il salto alla locazione dedicata solo se gli operandi di cmp sono uguali,quindi EBX = 11.



Abbiamo disegnato il nostro diagramma di flusso con le nostre tabelle. Abbiamo indicato con una linea verde il salto effettuato, mentre con una linea rossa il salto non effettuato.



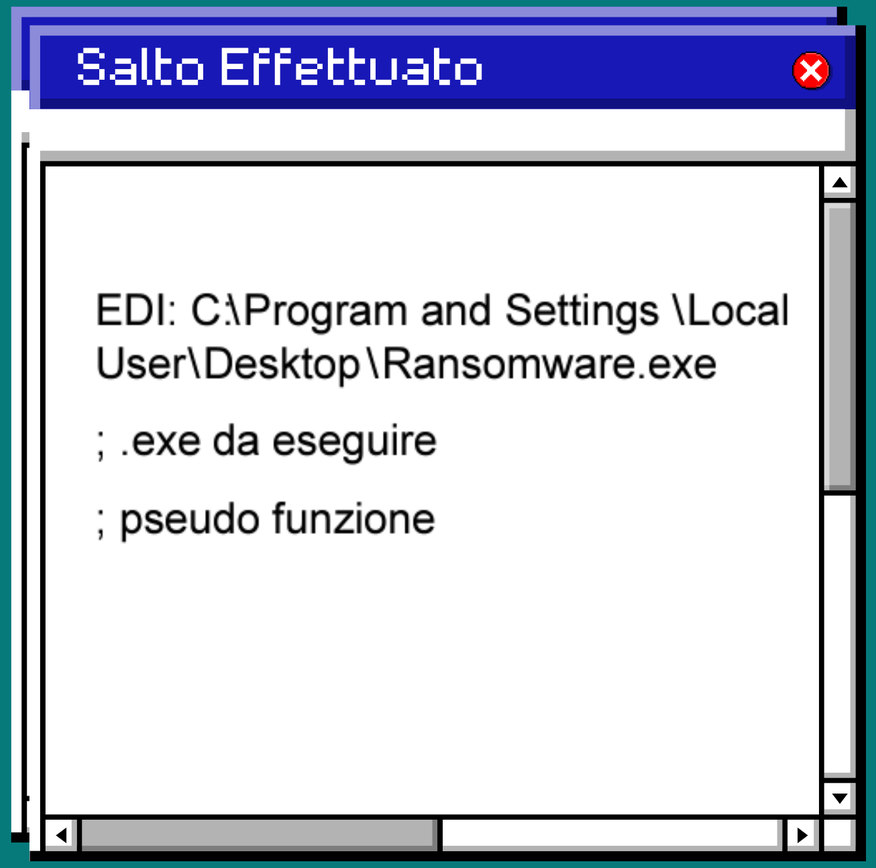




- Quali sono le diverse funzionalità implementate all'interno del Malware?

Possiamo dire che il Malware in questione implementa due funzionalità(di cui una sola eseguita):

1. Eseguire un Malware già presente sul PC,precedentemente scaricato probabilmente usando la funzione WinExec();[Salto Effettuato].
2. Scaricare un Malware da Internet,stiamo parlando probabilmente di un Downloader;[Salto Non Effettuato].



Torna alla pagina dell'indice

'Push'

- Push di dati: Prima di chiamare una funzione con l'istruzione call, è comune che vengano pushati i parametri necessari nello stack. Questi parametri possono includere variabili o altri dati che la funzione richiede per svolgere il suo compito.

'Call'

- Chiamata di funzione: Dopo che i dati sono stati pushati nello stack, l'istruzione call viene utilizzata per chiamare la funzione desiderata.

Esecuzione della funzione

- Dopo che è stata effettuata la chiamata alla funzione, il controllo passa alla funzione stessa. La funzione esegue le operazioni necessarie, accedendo ai dati pushati nello stack se necessario.

Argomenti delle funzioni 'Call'

Gli argomenti passati a un'istruzione call possono variare a seconda del tipo di chiamata e della convenzione di chiamata utilizzata, che può dipendere dall'architettura del processore e dalle convenzioni del compilatore.

Torna alla pagina dell'indice

In entrambe le funzioni i parametri sono passati sullo stack con l'istruzione 'Push'

WinExec()

L'argomento di questa funzione è il path(percorso) dell'eseguibile da innescare.

DownloadToFile()

L'argomento che viene dato a questa funzione invece è l'URL dove si possono scaricare altri file pregiudicati

Torna alla pagina dell'indice

Simone Forlenza

Paolo Di Maio

Grazie!

https://www.byterebels.eu/

Federico Tizzi

Davide Cannavacciuolo

Federico Russo