Progetto Settimana 11

Pablo Andres Balbuena Rios

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.

1 Traccia

- Possiamo notare che in questo codice ci sono due salti condizionali, il quale solo uno dei due viene effettuato.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	; EBX=10
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	; EBX=10+1=11
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

Un salto condizionale è un'istruzione di controllo di flusso in un programma che determina se eseguire o meno un salto in base alle condizioni del risultato di una precedente operazione.

L'istruzione di salto condizionale jz (Jump if Zero) è utilizzata per eseguire un salto ad un indirizzo specifico se il flag zero (ZF) è impostato. Il flag zero è impostato quando il risultato di un'operazione precedente è zero.

Il salto condizionale che viene effettuato si trova nell'indirizzo <<00401068>>, questo è dovuto al fatto che la sua condizione si è avverata, ovvero "i registri comparati sono uguali."

2 Traccia

jnz effettua un salto se il flag zero (ZF) non è impostato, ovvero quando i registri comparati non sono uguali.

jz effettua un salto se il flag zero (ZF) è impostato, ovvero quando i registri comparati sono uguali.

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	; EAX=5
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	; EBX=11
00401068	jz	loc 0040FFA0	; tabella 3

Non effettuato

effettuato

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

3 Traccia

In ognuna delle due tabelle possiamo notare una funzionalità:

- Tabella 2: In questa tabella notiamo che avviene uno scaricamento attraverso un URL di internet, normalmente i Malware che effettuano questa funzionalità sono dei Downloader.
- Tabella 3: Invece in questa tabella notiamo che esegue l'avvio di un file eseguibile "Ransomware.exe".

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

Un "Downloader" è un tipo di software o script progettato per scaricare un malware oppure un componente di esso da Internet per poi eseguirlo sul sistema target.

Il Ransomware è un tipo di malware progettato per crittografare i dati su un dispositivo o una rete, per poi chiedere un pagamento, in criptovaluta, in cambio della chiave di decrittazione.

4 Traccia

In entrambi le tabelle i parametri sono passati sullo stack utilizzando l'istruzione push.

Lo stack è una regione di memoria utilizzata nei programmi per la gestione delle chiamate di funzione.

- Tabella 2: In questa tabella il parametro passato è il registro "EAX", che contiene URL "www.malwaredownload.com".
- Tabella 3: Invece in questa tabella il parametro passato è il registro "EDX", che contiene il path del file eseguibile "C:\…\Ransomware.exe"

EAX ed EDX sono dei registri a 32 bit presenti nell'architettura dei processori x86 e x86-64

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

Un "Downloader" è un tipo di software o script progettato per scaricare un malware oppure un componente di esso da Internet per poi eseguirlo sul sistema target.

Il Ransomware è un tipo di malware progettato per crittografare i dati su un dispositivo o una rete, per poi chiedere un pagamento, in criptovaluta, in cambio della chiave di decrittazione.