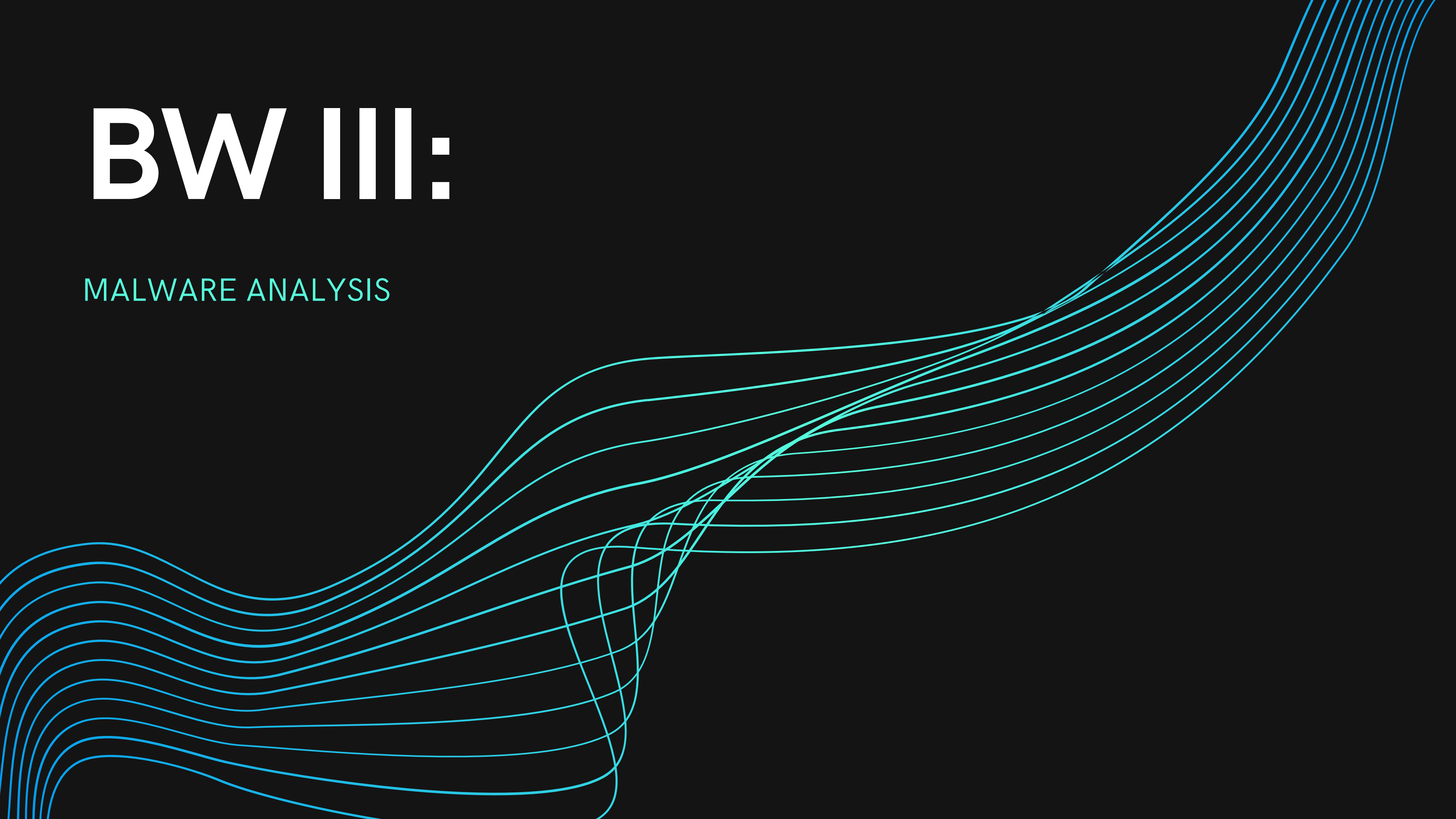


# BW III:

MALWARE ANALYSIS



# TRACCIA 1:

## 1° GIORNO

Con riferimento al file eseguibile

Malware\_Build\_Week\_U3, rispondere ai seguenti quesiti utilizzando le tecniche apprese nelle lezioni teoriche:

- Quanti parametri sono passati alla funzione Main()?
- Quante variabili sono dichiarate all'interno della funzione
- Quali sezioni sono presenti all'interno del file eseguibile?

Descrivete brevemente almeno 2 di quelle identificate

- Quali librerie importa il Malware ? Per ognuna delle librerie importate, fate della sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.



```
hModule= dword ptr -11Ch
```

```
(LPCSTR lpModuleName)
```

```
; LPVOID Str
```

```
: nSize
```

# MAIN:

## PARAMETRI:

Dall'analisi del Malware Building\_Week\_Unit\_3 possiamo identificare 5 parametri:

- DWORD: Che indica un intero senza segno di 32 bit
- HANDLE: Un particolare tipo di oggetto che punta a processi che sono stati aperti o creati
- LPCSTR: Un puntatore che punta ad una stringa
- LPVOID: Un puntatore che punta ad un void
- nSize: Un parametro che specifica la dimensione di un buffer

```
; int __cdecl main(int argc, const char **argv, const char **envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```





## VARIABILI:

Con riferimento allo screenshot possiamo individuare 3 diverse variabili:

- var\_117
- var\_8
- var\_4

E 2 argomenti:

- argc
- argv

Name	Start	End	R	W	X	D	L	Align	Base	Type	Class	AD	es	ss	ds	fs	gs
 .text	00401000	00407000	R	.	X	.	L	para	0001	public	CODE	32	0000	0000	0003	FFF...	FFF...
 .idata	00407000	004070DC	R	.	.	.	L	para	0002	public	DATA	32	0000	0000	0003	FFF...	FFF...
 .rdata	004070DC	00408000	R	.	.	.	L	para	0002	public	DATA	32	0000	0000	0003	FFF...	FFF...
 .data	00408000	0040C000	R	w	.	.	L	para	0003	public	DATA	32	0000	0000	0003	FFF...	FFF...

## SEZIONI:

- .text: Contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato
- .idata: Contiene informazioni sulle funzioni esterne che il programma importa da altre librerie o librerie a collegamento dinamico (DLL)
- .rdata: Include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile
- .data: Contiene tipicamente i dati - le variabili globali del programma eseguibile



Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

## LIBRERIE:

- KERNEL32.DLL: Contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria. Presenta 51 funzioni
- ADVAPI32.DLL: : Contiene le funzioni per interagire con i servizi ed i registri del sistema operativo. Presenta 2 funzioni

## FUNZIONI:

- RegCreateKeyExA: Che consente ai programmi di creare nuove chiavi all'interno del registro di sistema di Windows.
- RegSetValueExA: Che consente ai programmi di modificare o creare valori all'interno del registro di sistema

Queste sono le 2 Funzioni all'interno della libreria ADVAPI32

- VirtualAlloc: Potrebbe essere utilizzata per allocare memoria virtuale all'interno del processo corrente in cui eseguire il codice malevolo
- FindResourceA : Viene utilizzata per caricare risorse malevoli come codice aggiuntivo o immagini ingannevoli.
- GetCommandLineA: Il malware potrebbe utilizzarla per estrarre informazioni sensibili passate come argomenti al programma.
- GetProcAddress: per caricare funzioni dannose da librerie legittime già presenti sul sistema

Queste, invece, sono alcune delle funzioni trovate nella libreria KERNEL32

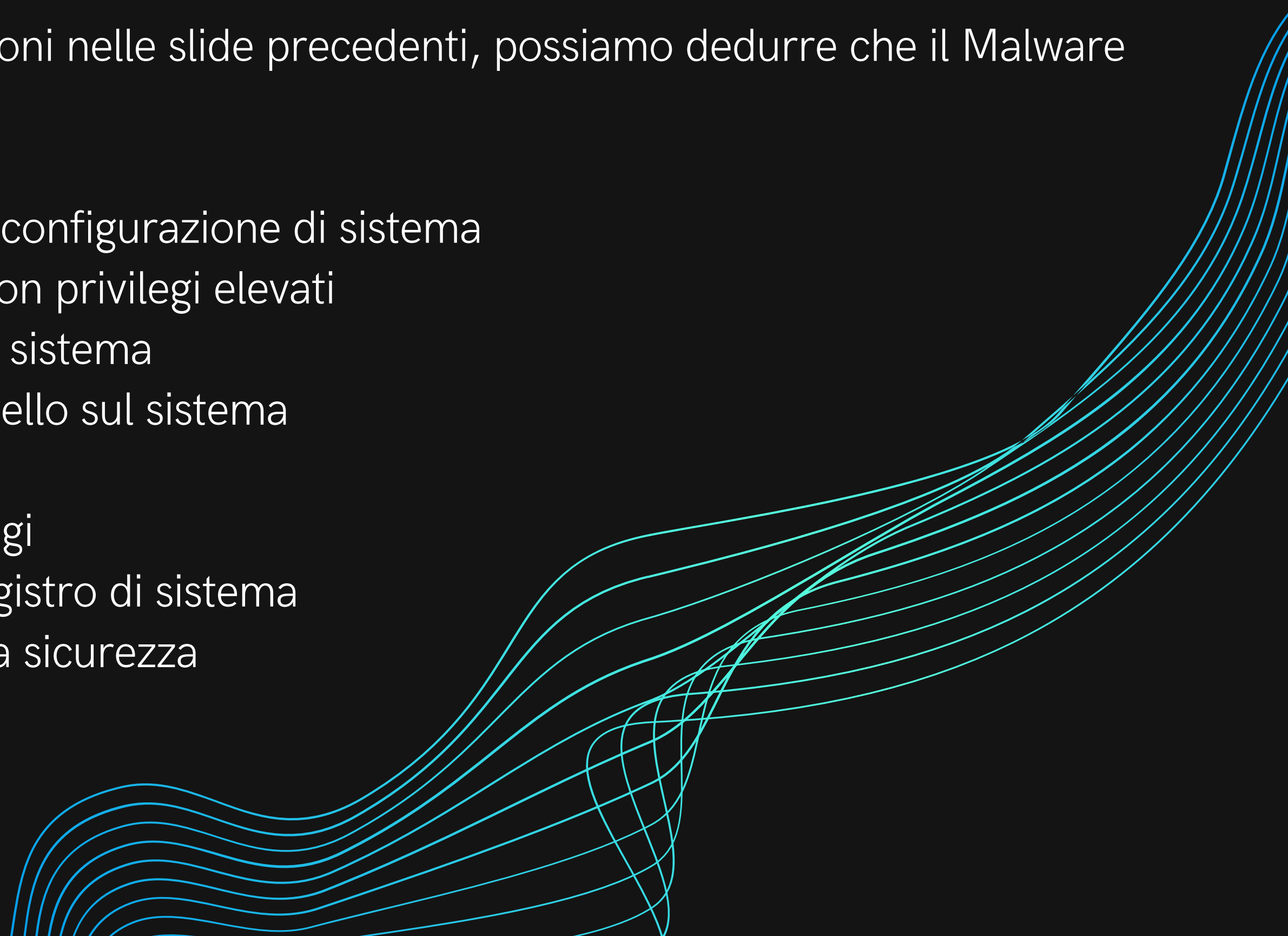
# CONCLUSIONE:

Identificate le due librerie e le funzioni nelle slide precedenti, possiamo dedurre che il Malware potrebbe tentare di:

(KERNEL32.DLL)

- Modificare le impostazioni o la configurazione di sistema
- Accedere a risorse di sistema con privilegi elevati
- Iniettarsi in processi o servizi di sistema
- Eseguire operazioni di basso livello sul sistema

(ADVAPI32.DLL)

- Gestire account utente e privilegi
  - Eseguire operazioni su file e registro di sistema
  - Accedere a funzioni relative alla sicurezza
- 
- A series of thin, light blue wavy lines that originate from the bottom left and curve upwards and to the right, creating a sense of motion and flow across the bottom half of the slide.



# GRAZIE PER L'ATTENZIONE

