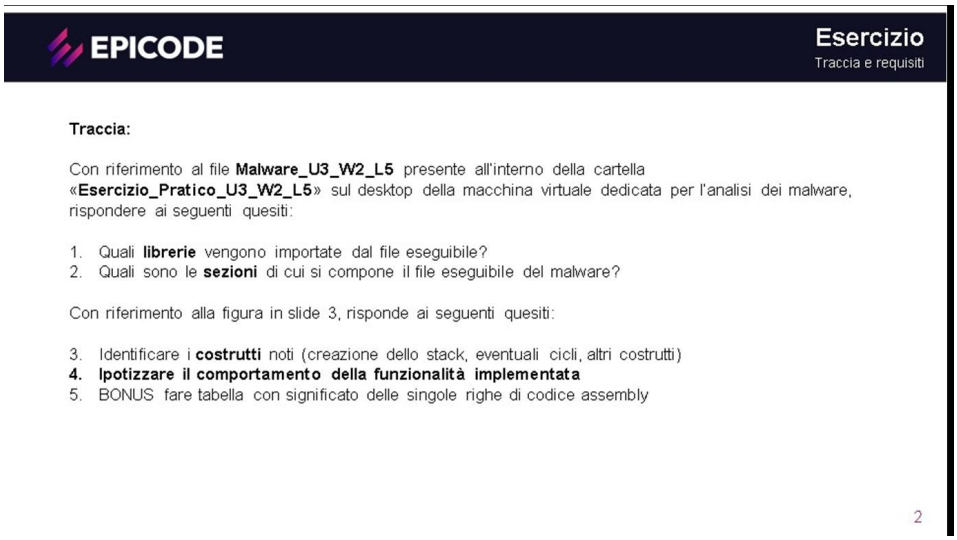
PROGETTO S10 L5



EPICODE

Esercizio
Traccia e requisiti

Traccia:

Con riferimento al file **Malware_U3_W2_L5** presente all'interno della cartella «**Esercizio_Pratico_U3_W2_L5**» sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

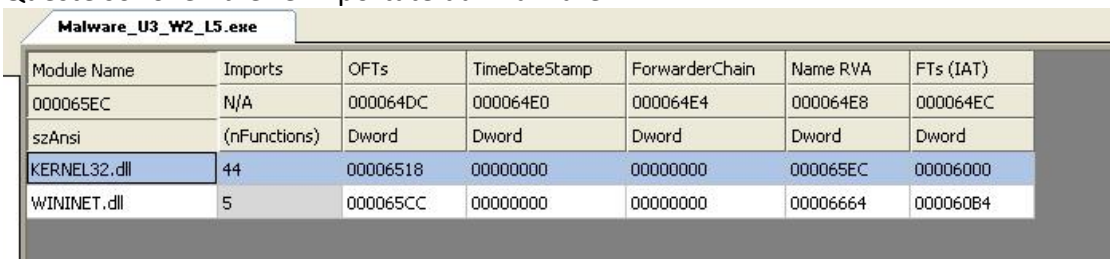
1. Quali **librerie** vengono importate dal file eseguibile?
2. Quali sono le **sezioni** di cui si compone il file eseguibile del malware?

Con riferimento alla figura in slide 3, risponde ai seguenti quesiti:

3. Identificare i **costrutti** noti (creazione dello stack, eventuali cicli, altri costrutti)
4. **Ipotizzare il comportamento della funzionalità implementata**
5. BONUS fare tabella con significato delle singole righe di codice assembly

2

Queste sono le librerie importate dal malware.

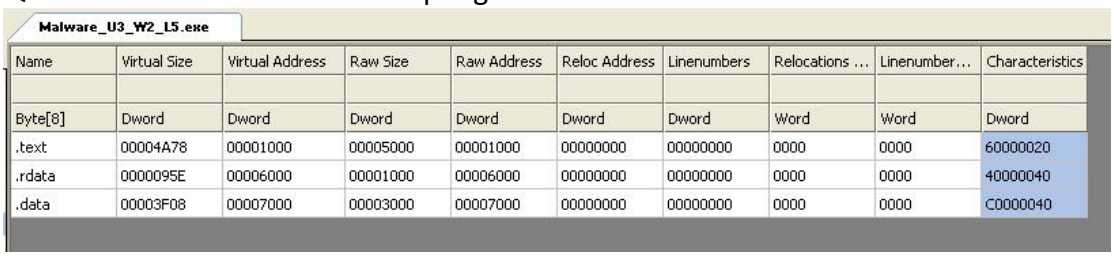


Malware_U3_W2_L5.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000065EC	N/A	000064DC	000064E0	000064E4	000064E8	000064EC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

- Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria.
- Wininet.dll:contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Queste sono le sessioni che compongono il malware.

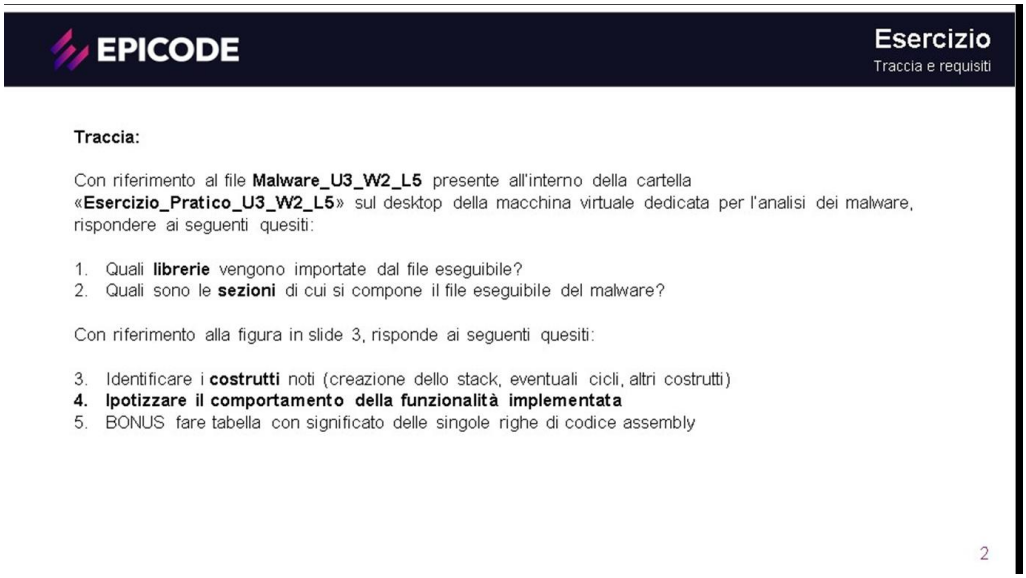


Malware_U3_W2_L5.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

.text: contiene le istruzioni che la CPU eseguirà una volta che il software sarà avviato.
.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, che devono essere disponibili da qualsiasi parte del programma.

PROGETTO S10/L5



//INIZIALIZZAZIONE DI STACK

push ebp --> implementazione di EBP nello stack
mov ebp, esp --> valorizzazione del puntatore stack = EBP

//PREPARAZIONE DELLA FUNZIONE

push ecx --> implementazione di ECX nello stack
push 0 ;dwReserved --> impl di dwReserved a valore 0
push 0 ;lpdwFlags --> impl di lpdwFlags a valore 0
call ds:InternetGetConnectedState --> chiamata funzione per il collegamento a internet, restituisce valori booleani

//CONFRONTO PER COMINCIARE IL CICLO

mov [ebp+var_4], eax --> presa in carico del valore creato dalla funzione
cmp [ebp+var_4], 0 --> comparazione del valore per la creazione di un flag
jz short loc_40102B --> salta se ZF = 0

----- ciclo if-else, se ZF = 0 SALTA AL ERROR, ALTRIMENTI SUCCESO ----

//sucs internet connection --> ZF = 1

push offset aSuccessInterne ; “Success: Internet Connection\n”
call sub_40105F --> richiamo funzione
add esp, 4 --> esp +4
inc eax, 1 --> incremento di eax +1
jz short loc_40103A --> salta se ZF = 0 al end

//err int conn --> ZF = 0

loc_40102B: ; "Error 1.1: No Internet\n"
push offset aError1_1NoInte --> La stringa di errore viene caricata sullo stack
call sub_40117E --> richiamo funzione
add esp, 4 --> esp +4
xor eax,eax --> azzeramento di eax

//end

```
loc_40103A:
mov     esp, ebp        ------v
pop     ebp             --> pilizia dello stack
retn                    --> fine
sub_401000 endp         --> ritorno al inizio
```

***** IPOTESI COMPORTAMENTO *****

Questo codice ci suggerisce che il malware in questione tenta la connessione a internet.
le momento i cui ha successo svolge una determinata funzione che non è presente nel esercizio
mentre che nel momento in cui non si collega invia errore e resetta il puntatore
e nel end resetta tutti i valori e l'ultima righa indica un ritorno alla cima, un ricomincio.