

The background features a dark blue gradient with three glowing, translucent 3D torus shapes. One ring is positioned on the left side, another on the right side, and a third, larger ring is at the bottom left corner.

S10L5

Malware Analysis

Roadmap

1

Traccia

4

Analisi
costrutti

2

Analisi
librerie

5

Conclusioni

3

Sezioni
malware

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:

- Quali librerie vengono importate dal file eseguibile?
- Quali sono le sezioni di cui si compone il file eseguibile del malware?
- Con riferimento alla figura in slide 3, risponde ai seguenti quesiti: Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti)
- Ipotizzare il comportamento della funzionalità implementata

Analisi librerie



L'analisi delle librerie è una parte importante del processo di analisi del malware.

Questo processo è volto a identificare e comprendere le funzioni chiamate o importate da un malware durante la sua esecuzione, permettendoci di comprendere alcuni possibili funzionamenti del malware ancor prima di avviarlo.



- Analisi librerie

CFF Explorer

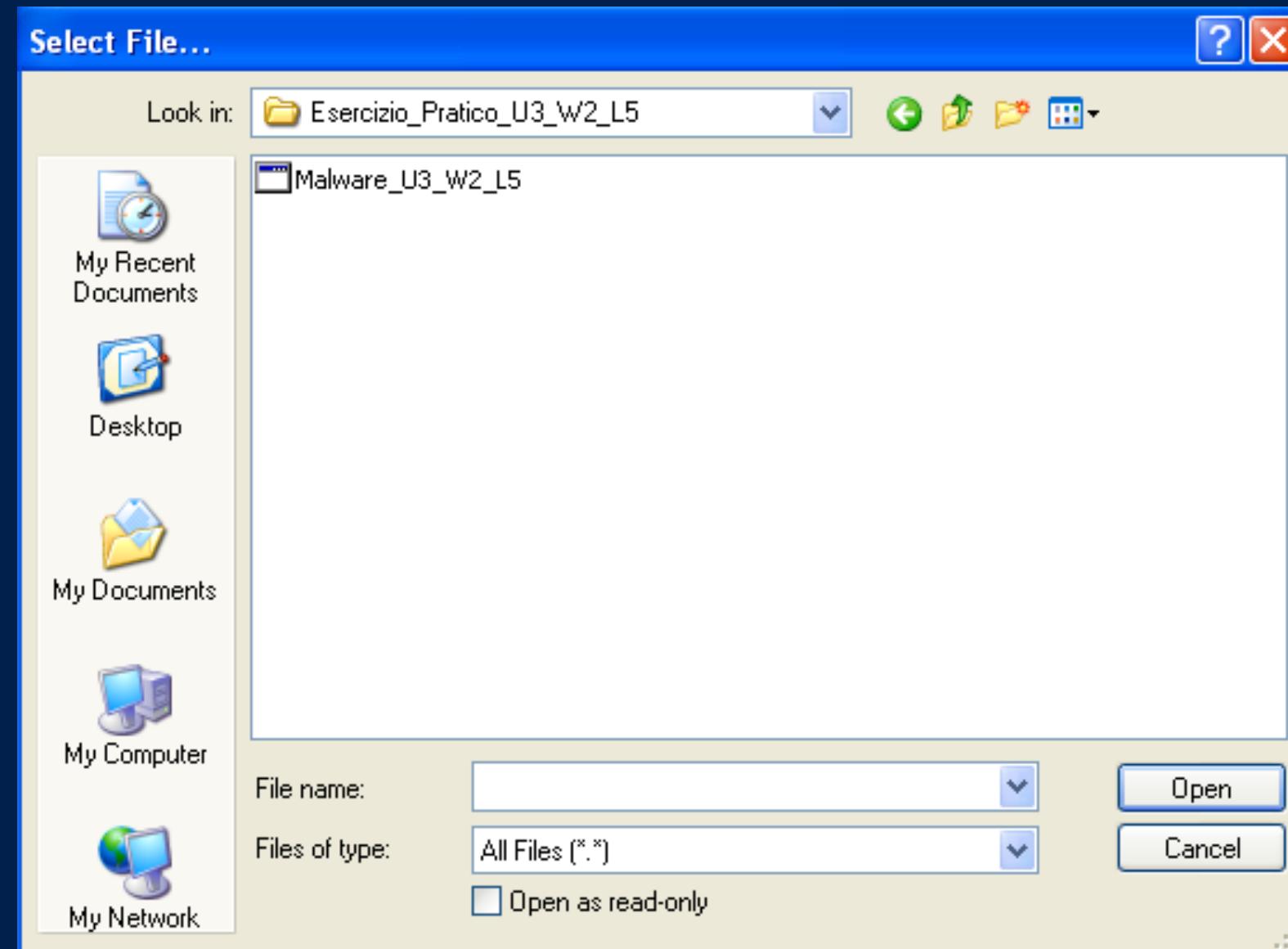
Per l'analisi di oggi utilizzeremo ***CFF Explorer***, un software gratuito e avanzato di esplorazione di file PE (Portable Executable). È utilizzato principalmente per analizzare e modificare file eseguibili in formato PE, come eseguibili Windows (EXE), dynamic link libraries (DLL) e altri formati correlati.



Icona del
programma



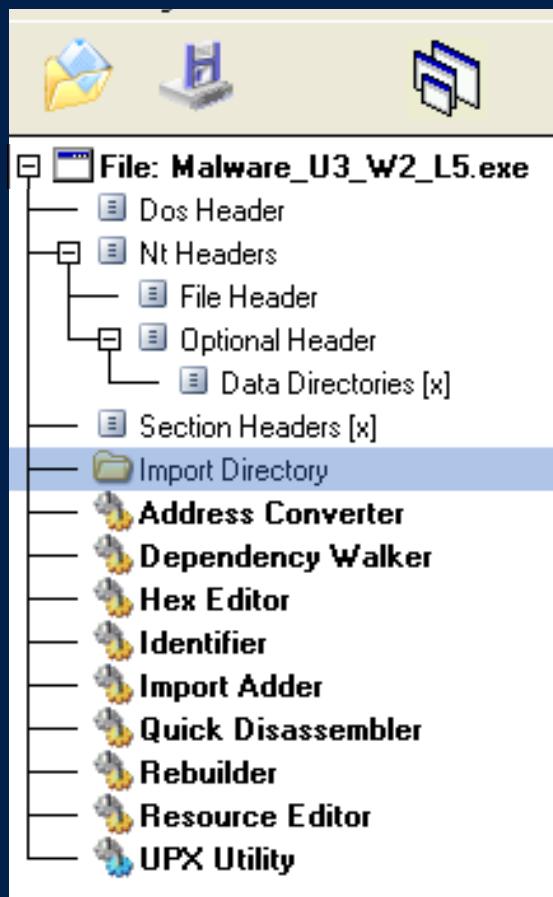
- Analisi librerie



Una volta aperto CFF
Explorer importiamo
l'eseguibile del malware al
suo interno e clicchiamo
“Open”



- Analisi librerie



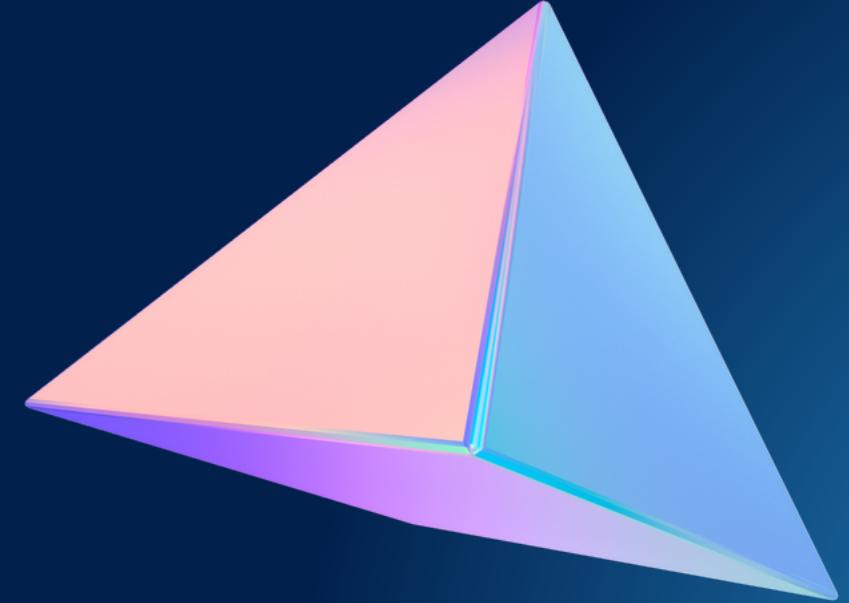
Come da immagine,
le librerie importate
da questo malware
sono “KERNEL32.dll”
e “WININET.dll”

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

dopodiché, tramite il menù a sinistra
clicchiamo la voce “import directory”
che mostrerà la schermata seguente



Approfondimento: **DLL**



un "Dynamic Link Library" o DLL è un tipo di file eseguibile in ambiente Windows che contiene codice e dati che possono essere utilizzati da più programmi contemporaneamente.

A differenza di un'applicazione autonoma, una DLL non può essere eseguita direttamente, ma fornisce funzionalità condivise che possono essere richiamate da diverse applicazioni.



kernel32.dll:

- Fornisce funzioni di basso livello che gestiscono memoria, file, processi e altri aspetti fondamentali del sistema operativo.
- Include funzioni per la gestione dei processi, sincronizzazione, allocazione di memoria e la gestione delle eccezioni.
- È una delle DLL principali di Windows e molte altre DLL fanno riferimento a sue funzioni

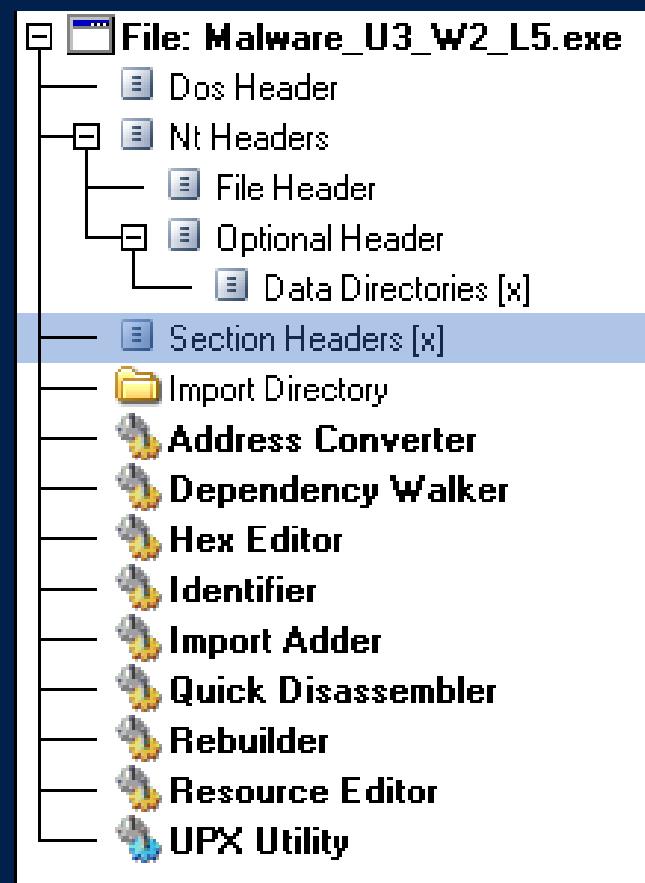
winnet.dll:

- Offre funzioni per la gestione delle operazioni di rete, inclusi protocolli come HTTP, FTP e altri.
- È coinvolta nella gestione delle connessioni Internet e fornisce un'interfaccia per le operazioni di navigazione e download.
- Utilizzata da molti programmi per interagire con il Web e le risorse Internet.

Sezioni malware

Il codice del malware in questione, come ogni eseguibile windows, è diviso in diverse sezioni ognuna con la sua funzione specifica.

- Sezioni Malware



Sempre dallo stesso menù di CFF
Explorer è possibile accedere alla voce
“Section Headers” e così visualizzare le
sezioni dell'eseguibile

Le sezioni trovate sono:

.text

.rdata

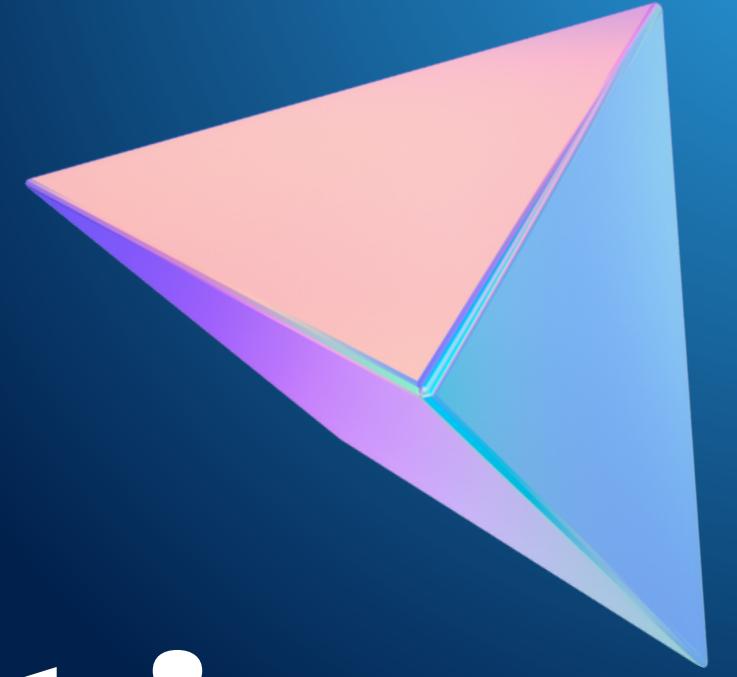
.data

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber... Characteristics	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: La sezione "text" comprende le istruzioni, ovvero le linee di codice, che la CPU eseguirà una volta avviato il software. Di solito, questa è l'unica sezione di un file eseguibile che la CPU esegue, poiché tutte le altre sezioni contengono dati o informazioni di supporto.

.rdata: La sezione "rdata" contiene informazioni sulle librerie e sulle funzioni importate o esportate dall'eseguibile.

.data: La sezione "data" contiene i dati o le variabili globali del programma eseguibile. Si noti che una variabile viene considerata globale quando non è definita all'interno del contesto di una funzione, ma è dichiarata globalmente e, di conseguenza, è accessibile da qualsiasi funzione dell'eseguibile.



Analisi costrutti

Questa sezione si occupa di analizzare i costrutti assembly all'interno del malware, spiegando il loro funzionamento.



I costrutti trovati sono stati evidenziati in immagine

```
push    ebp  
mov     ebp, esp  
push    ecx  
push    0          ; dwReserved  
push    0          ; lpdwFlags  
call    ds:InternetGetConnectedState  
mov     [ebp+var_4], eax  
cmp     [ebp+var_4], 0  
jz      short loc_40102B
```

Creazione dello stack

Costrutto IF

```
push    offset aSuccessInterne ; "Success: Internet Connection\n"  
call    sub_40117F  
add    esp, 4  
mov    eax, 1  
jmp    short loc_40103A
```

```
loc_40102B:           ; "Error 1.1: No Internet\n"  
push    offset aError1_1NoInte  
call    sub_40117F  
add    esp, 4  
xor    eax, eax
```

```
loc_40103A:  
mov    esp, ebp  
pop    ebp  
retn  
sub_401000 endp
```

Rimozione dello stack

Conclusioni

All'interno del codice assembly assegnato ci sono molti indizi sul funzionamento di questo malware. Esso infatti richiama una funzione della libreria wininet32, “InternetGetConnectedState”, ovvero controlla se la macchina in cui viene avviato l'eseguibile è connessa ad internet o meno. Tramite il costrutto if posto subito dopo il malware da due possibili risultati a seconda della presenza di questa connessione:

Se la connessione è presente passa come parametro “Success: internet connection”

altrimenti “Error 1.1: no internet”

Con tutta probabilità queste stringhe vengono passate come parametri ad un secondo eseguibile, che verifica che la macchina bersaglio sia connessa ad internet prima di attuare un attacco/connessione malevola.