

# S10-L1

(Bonaldi Cristian)



---

## Malware analysis - Analisi statica basica

### Traccia:

Con riferimento al file eseguibile contenuto nella cartella

«Esercizio\_Pratico\_U3\_W2\_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

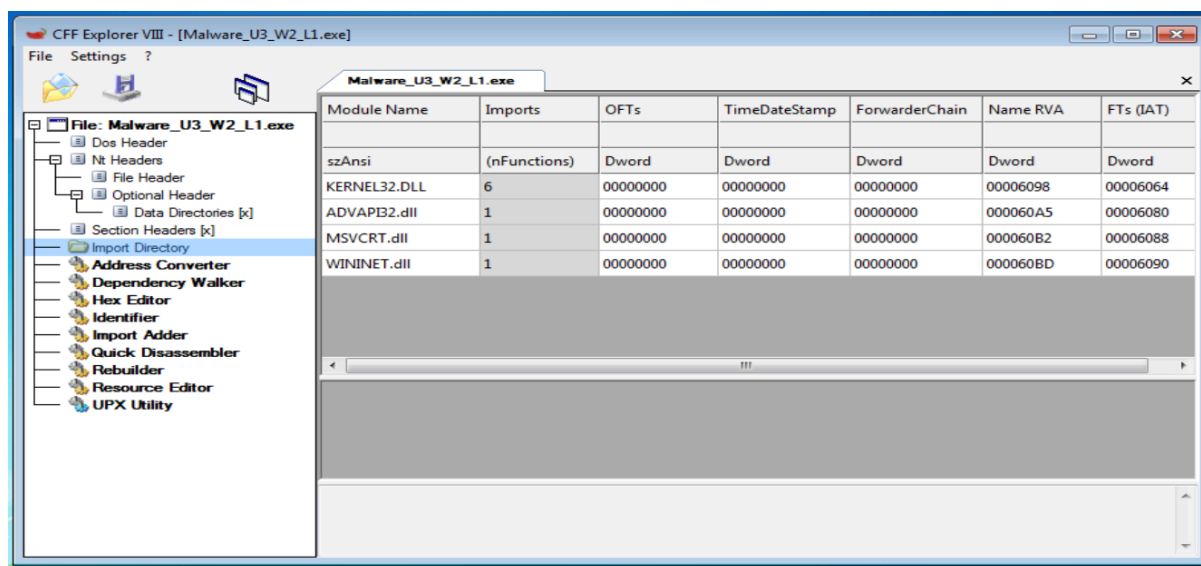
- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

---

### Esercizio e sviluppo:

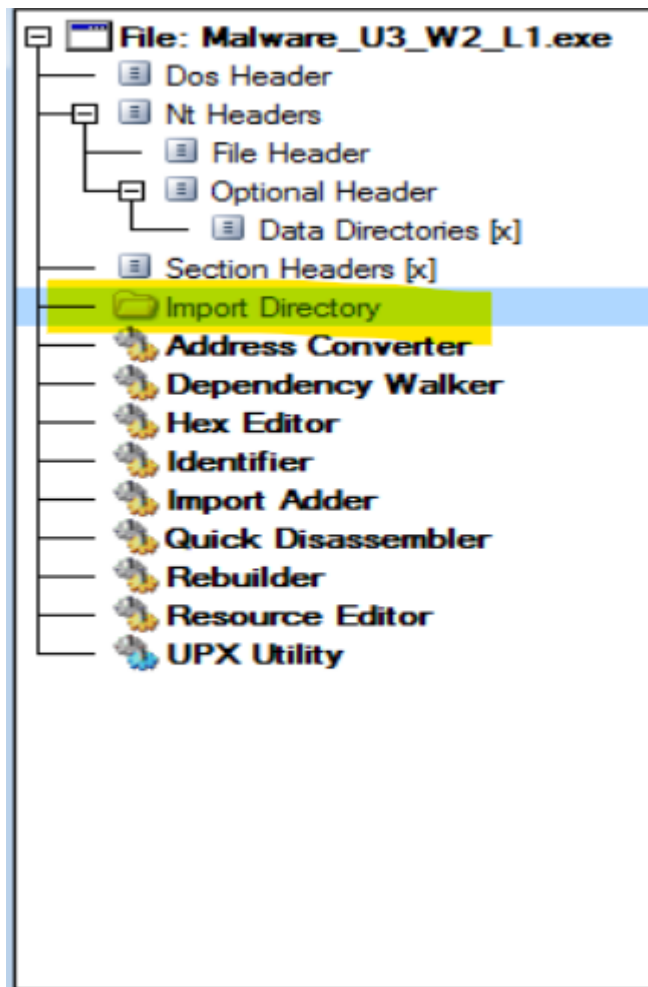
1.

Per prima cosa, importiamo Windows7 per l'analisi dei malware su Virtual Box e avviamo CFF Explorer all'interno della macchina.



Dopodiché apriamo il file Malware\_U3\_W2\_L1.exe per l'analisi statica e ci dirigiamo nella sezione **Import Directory** per visualizzare l'elenco delle librerie DLL importate.

Una **DLL** (Dynamic-Link Library) è un tipo di file che contiene codice e dati che possono essere utilizzati da più programmi contemporaneamente. In sostanza è una raccolta di funzioni e risorse che i programmi possono caricare ed eseguire o includere direttamente nei loro file eseguibili. Queste sono essenziali per l'analisi dei malware poiché aiutano a scoprire le operazioni malevole utilizzate dal codice infetto. Analizzando le DLL usate, si può capire come si comporta il malware in questione. Questo può includere cose come modificare i processi di sistema, comunicare con server esterni o cambiare le impostazioni del Registro di sistema.



Come si può notare, individuiamo le seguenti librerie:

Malware_U3_W2_L1.exe						
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

**-KERNEL32.DLL:** questa è una libreria di sistema di Windows che offre funzioni fondamentali per le operazioni di base del sistema operativo. È una delle librerie principali che i programmi utilizzano per comunicare con il sistema operativo e svolgere compiti

essenziali come gestire la memoria, creare e controllare processi e leggere o scrivere dati su file.

**-ADVAPI32.dll:** è una libreria di sistema di Windows che fornisce un insieme di funzioni avanzate utilizzate dai programmi per eseguire operazioni critiche come la gestione del Registro di sistema, la sicurezza del sistema, il controllo degli accessi e la gestione dei servizi di sistema.

**-MSVCRT.dll:** è una libreria di Microsoft inclusa nel Microsoft Visual C Runtime, ovvero un insieme di librerie che fornisce ai programmi scritti in C e C++ delle funzioni e servizi fondamentali e offre strumenti che si possono sfruttare per fare operazioni comuni senza dover riscrivere tutto da zero.

**-WININET.dll:** è una libreria di Windows dedicata alla gestione dell'accesso a Internet. Essa offre tutte le funzioni necessarie per lavorare con vari protocolli di rete, rendendo più semplice la comunicazione tra i programmi e i servizi web.

2.

All'interno della schermata **Section Headers** di CFF Explorer, si può vedere la struttura delle sezioni che compongono il malware. Queste sezioni forniscono informazioni importanti riguardo l'organizzazione del file eseguibile e a come si comporta quando è caricato in memoria. In questo caso, le tre sezioni del malware appaiono in questo modo:

Malware_U3_W2_L1.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	00000248	0000024A	0000024C
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Questo significa che siamo di fronte ad un file compresso tramite UPX (Ultimate Packer for Executables). In pratica UPX è un programma open source molto usato per comprimere file eseguibili, riducendone le dimensioni.

Analizzando le tre sezioni del malware possiamo notare:

**UPX0:** contiene i dati che sono stati compressi da UPX. In alcuni casi, potrebbe anche essere vuota

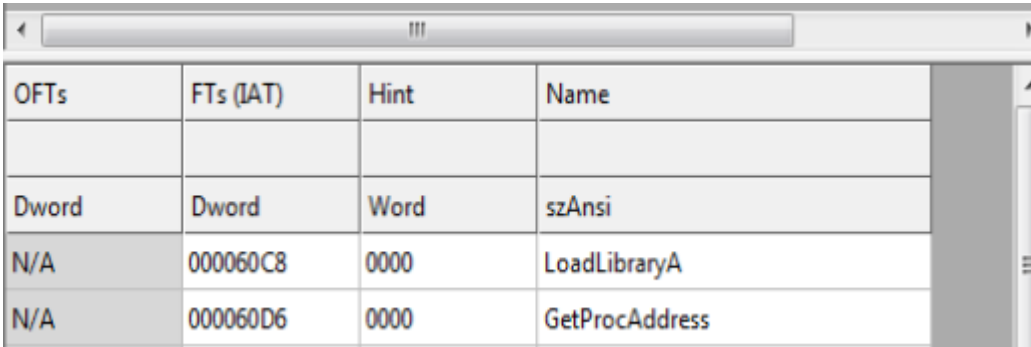
**UPX1:** questa è la sezione principale che contiene il codice dell'eseguibile.

**UPX2:** può contenere dati extra o servire ad altri scopi specifici. Non sempre è presente, ma quando c'è, potrebbe contenere altre parti di codice.

---

### 3.

In conclusione, possiamo affermare che ci troviamo di fronte a un malware evoluto che rende difficile ottenere dettagli rilevanti tramite una semplice analisi statica. Lo si capisce dalla presenza di funzioni come "LoadLibrary" e "GetProcAddress", che indicano un metodo usato spesso dai malware più complessi: le librerie vengono caricate solo durante l'esecuzione, rendendo difficile capire in anticipo quali librerie saranno effettivamente utilizzate. Questa tecnica permette al malware di sfuggire alle analisi standard e di nascondere meglio le sue vere operazioni, richiedendo metodi di analisi più sofisticati per capirne appieno il funzionamento.



OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress