Analisi statica basica

Prepared by

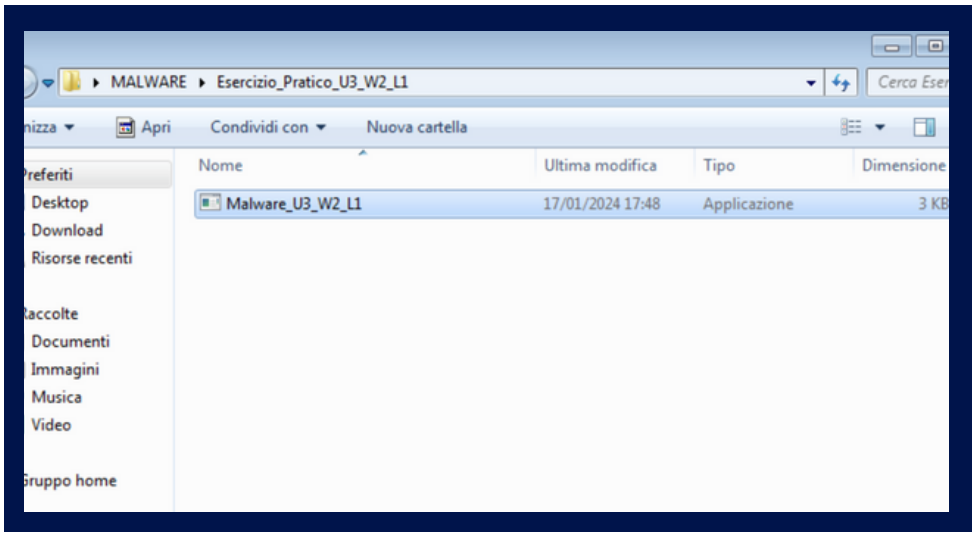
Alessandro Marasca

Presented to

Epicode - CS0124
S10L1

INDICE

TRACCIA



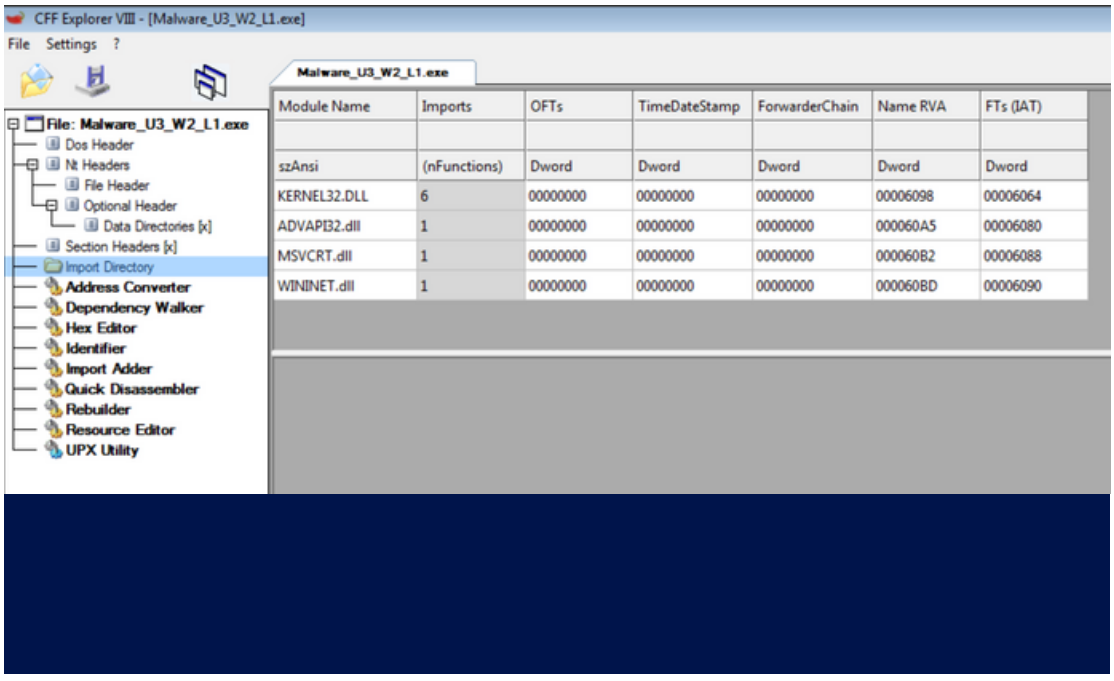
Con riferimento al file eseguibile contenuto nella cartella **«Esercizio_Pratico_U3_W2_L1»** presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- **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.

LIBRERIE IMPORTATE

Possiamo osservare le librerie importate in “**import directory**” , trovando:

1. **Kernel32.dll** (funzioni core del sistema operativo)
2. **Advapi32.dll** (per interagire con registri e servizi Windows)
3. **MSVCRT.dll** (manipolazioni scritte o allocazione memoria)
4. **Wininet.dll** (per implementare i servizi di rete come ftp, ntp, http)

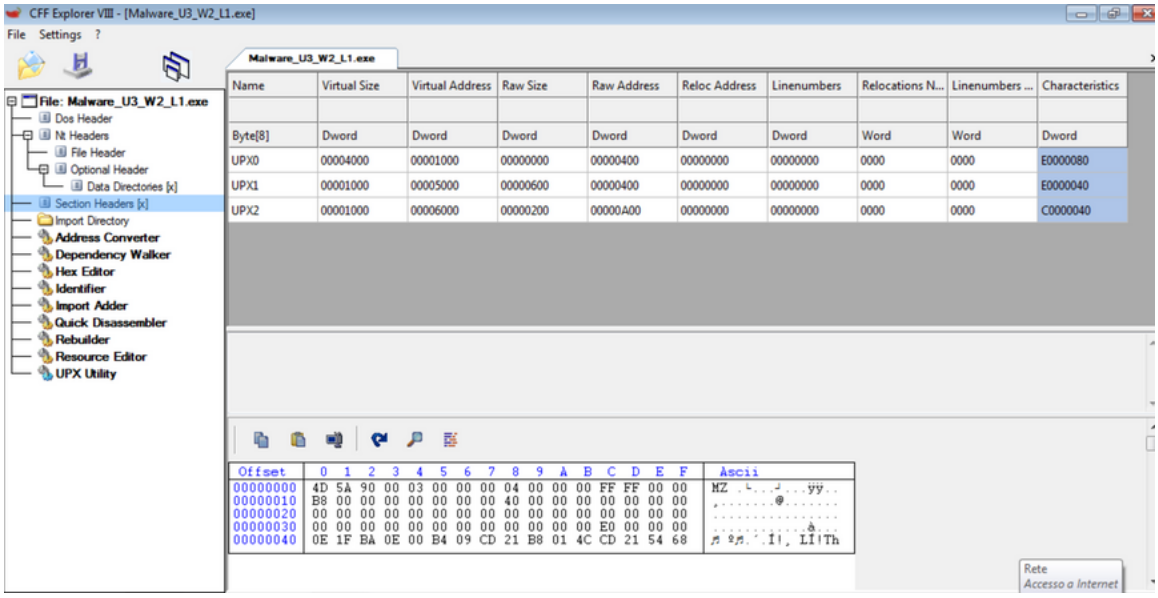


SEZIONI

Nella “**Section Headers**“ troviamo le sezioni del malware: sono 3 e sono:

1. **UPx0**
2. **UPx1**
3. **UPx2**

Non riusciamo però a trovare altre informazioni e quindi a fornire una descrizioni per le sezioni interessate.



CONSIDERAZIONI FINALI

Il malware analizzato in quest’operazione è avanzato: non riusciamo infatti ad identificare gli elementi e le librerie che lo compongono, poiché nascoste.

GRAZIE

Analisi statica basica

Prepared by
Alessandro Marasca

Presented to
Epicode - CS0124
S9L4