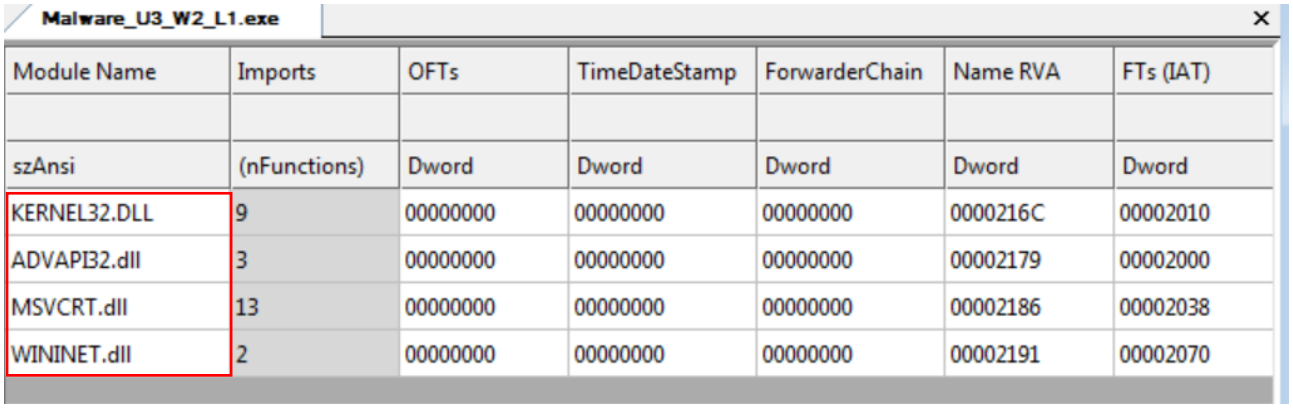
CONSEGNA SETTIMANA 10 LEZIONE 1

Analisi statica di un malware

---

*Il progetto di oggi prevede **l'analisi statica** di un malware. Per il nostro scopo useremo una VM preimpostata di windows 7 e il software **CFF Explorer**.*

Vediamo come si compone il malware.

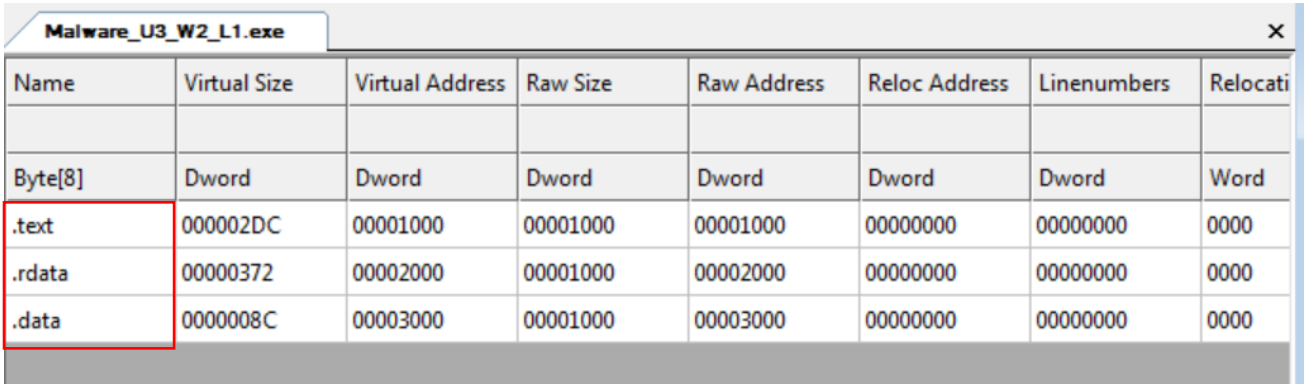


Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	9	00000000	00000000	00000000	0000216C	00002010
ADVAPI32.dll	3	00000000	00000000	00000000	00002179	00002000
MSVCRT.dll	13	00000000	00000000	00000000	00002186	00002038
WININET.dll	2	00000000	00000000	00000000	00002191	00002070

In questa sezione possiamo notare le varie librerie importate dal malware durante l'esecuzione, tra cui:

- **KERNEL32.dll –** la libreria kernel32 contiene le informazioni e le funzioni necessarie per far sì che il malware interagisca con il SO.
- **ADVAPI32.dll –** la libreria advapi32 contiene le informazioni e le funzioni per interagire con i servizi e i registri del SO.
- **MSVCRT.dll –** la libreria msvcert contiene le funzioni per poter manipolare le stringhe, allocare la memoria e sfruttare le operazioni di I/O.
- **WININET.dll –** la libreria wininet contiene le funzioni per implementare alcuni protocolli di rete (ad esmpio HTTP, FTP, e NTP).



Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocati
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000

Possiamo inoltre suddividere il malware in determinate sezioni, tra cui:

- **.text –** la sezione text contiene le istruzioni che verranno eseguite dalla CPU, dopo aver avviato il malware.
- **.rdata –** la sezione rdata contiene informazioni riguardanti le librerie e le funzioni importate ed esportate del malware.
- **.data –** la sezione data contiene le variabili globali del malware. *Per variabile globale si intende una variabile che non è limitata e definita in una funzione ma dichiarata globalmente, in modo da poter accederci da qualsiasi funzione del malware.*

Facciamo alcune considerazioni finali.

Da questa breve analisi non ci è dato sapere il preciso funzionamento del malware ma possiamo supporne il comportamento durante la sua esecuzione tramite le librerie.

Date le librerie **kernel32** e **msvcrt** si può ipotizzare che il malware interagisce con i file presenti all'interno del sistema operativo o possa richiamare altri software al suo interno. Si può anche supporre che tramite la libreria **advapi32** vada a modificare alcune voci nel registro di sistema. Infine possiamo immaginare che abbia anche una funzione dal lato della rete, in quanto tramite la libreria **wininet** sono implementati alcuni protocolli come l'HTTP.