Malware analysis

Sommario

Traccia S10/L1

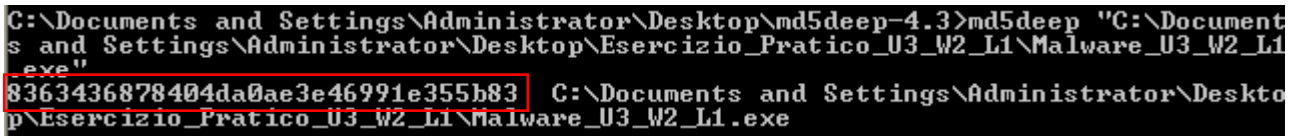
Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- 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

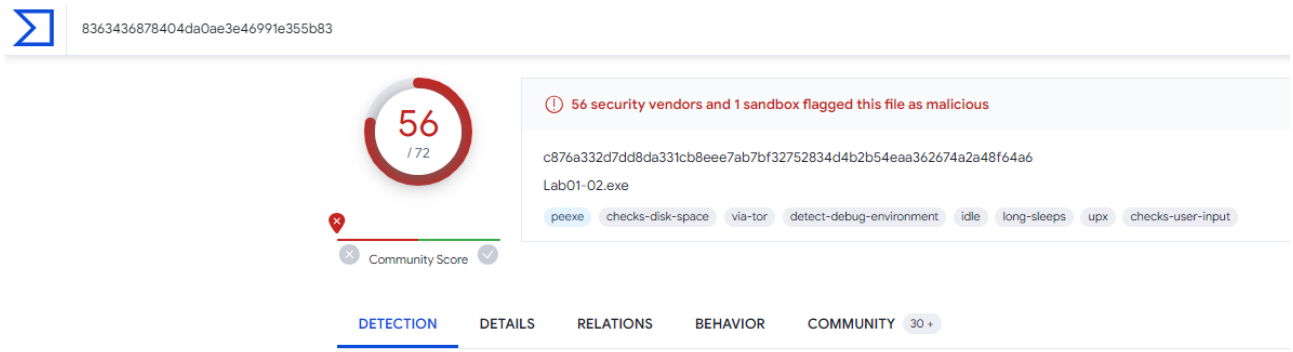
Verifica dell'eseguibile

Per verificare se l'eseguibile indicato nella traccia è effettivamente un malware calcoliamo l'hash tramite md5deep, una utility da riga di commando. L'hash è una stringa alfanumerica univoca che identifica un file, in pratica un'impronta digitale.

Avviamo il command prompt e cambiamo directory con quella contenente l'utility. Inseriamo il comando **md5deep "path del file da hashare".**

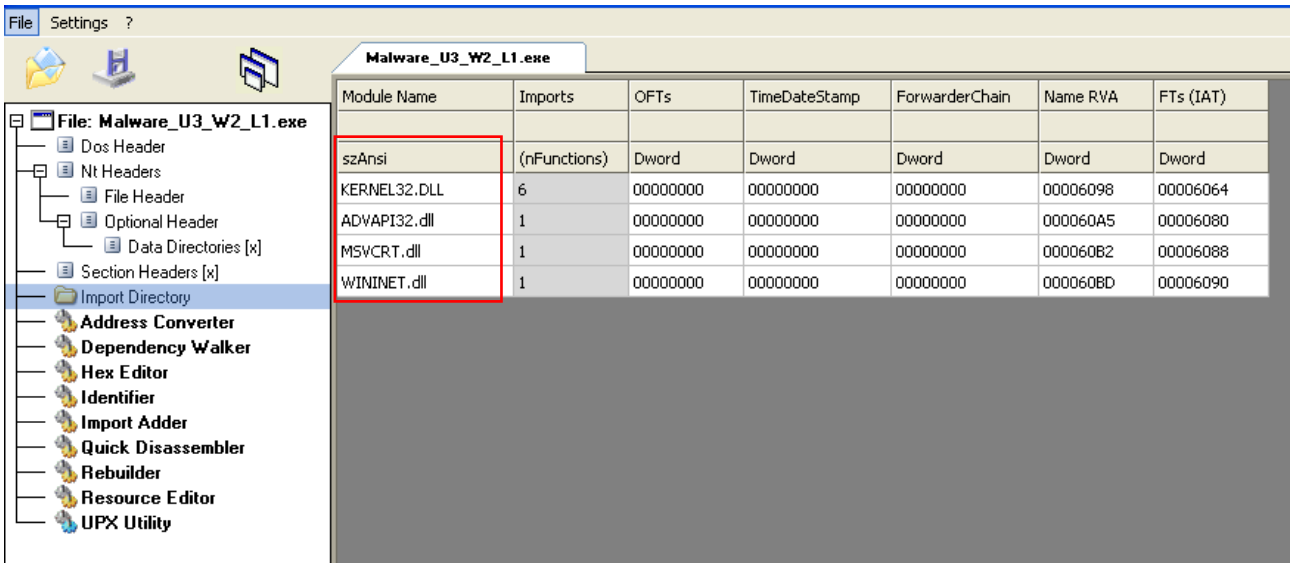


Ora che abbiamo ottenuto l'hash possiamo ricercalo su Virus Total, che mi indica che è un file malevolo.



Analisi librerie

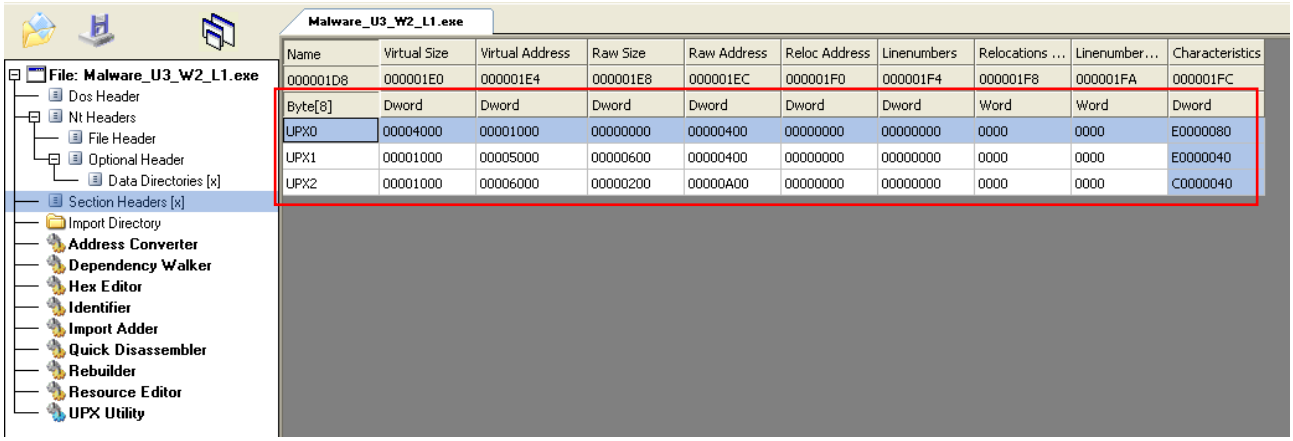
Per analizzare le librerie utilizziamo CFF Explorer. Le librerie sono un insieme di funzioni presenti nel sistema operativo che possono essere richiamate da un software



- KERNEL32.DLL: contiene le funzioni principali per interagire con il sistema operativo
- ADVAPI32.DLL: contiene le funzioni per interagire con i servizi e registri del sistema operativo
- MSVCRT.DLL: contiene funzioni per la manipolazione stringhe, allocazione memoria, chiamate per input/output in stile linguaggio C.
- WININET.DLL: contiene le funzioni per l'implementazione di protocolli di rete come HTTP, FTP, NTP

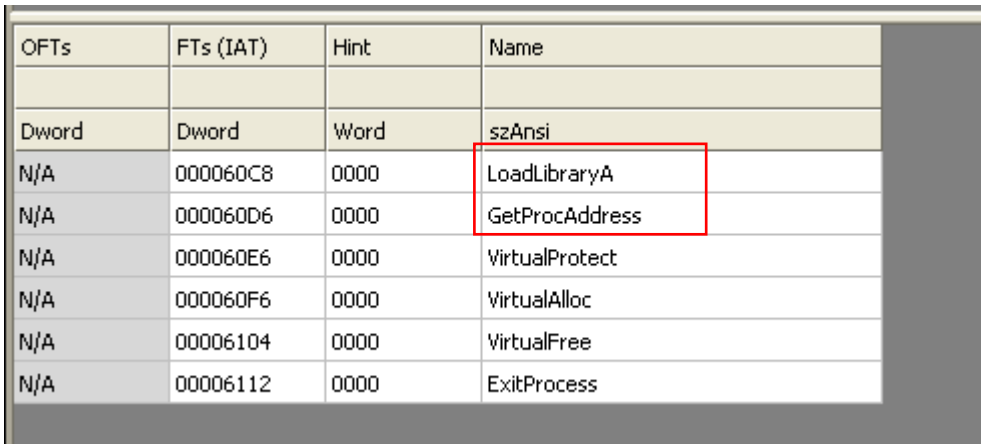
Analisi sezioni

Per analizzare le sezioni dell'eseguibile spostiamoci nella sezione Section Headers.



L'eseguibile è composto di 3 sezioni. Il nome di queste non è standard (di solito possiamo trovare .text, .data, .rsrc etc…), e questo è un indicatore di impacchettamento, sfruttato dal threat actor per nascondere il tipo di sezione. UPX sta per Ultimate Packer for eXecutables, un programma di compressione di eseguibili open source gratuito.

Tra le funzioni importate dalla libreria KERNEL32.DLL possiamo notare **LoadLibraryA** e **GetProcAddress**, che vengono appunto utilizzate per caricare funzioni addizionali durante l'esecuzione.



OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

Considerazioni finali

Con l'analisi statica basica non è possibile stabilire la natura di questo malware, dato che importa le librerie quando è in esecuzione. Con un'analisi dinamica sarà possibile estrapolare più informazioni.