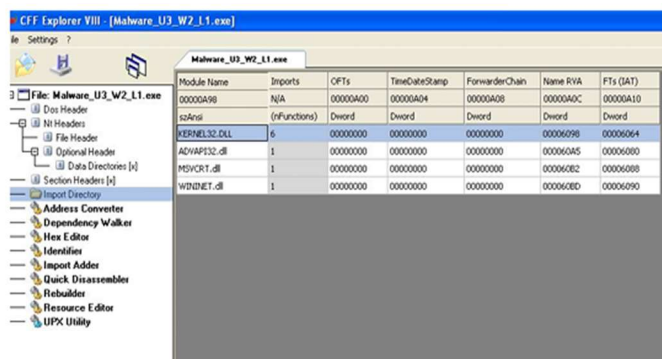


### Soluzione – Import librerie

Utilizzando CFF Explorer, vediamo dalla sezione import directory che il malware U3\_W2\_L1 importa 4 librerie:

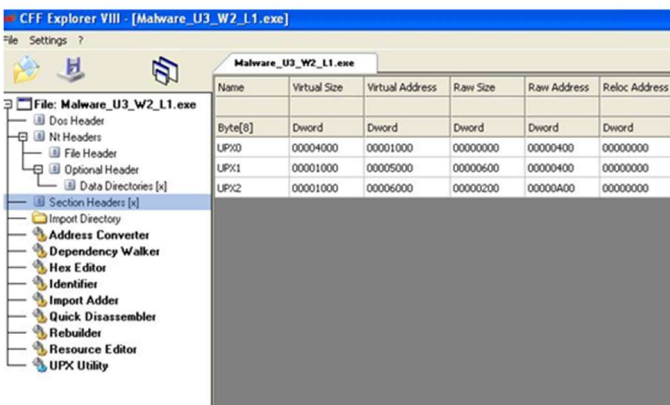
- ❑ **Kernel32.dll**, che include le funzioni core del sistema operativo
- ❑ **Advapi32.dll**, che include le funzione per interagire con registri e servizi Windows
- ❑ **MSVCRT.dll**, libreria scritta in C per la manipolazione scritte o allocazione memoria
- ❑ **Wininet.dll**, include le funzione per implementare i servizi di rete come ftp, ntp, http



Module Name	Imports	OFIs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
Kernel32.dll	6	00000000	00000000	00000000	00006098	000060A4
AdvAPI32.dll	1	00000000	00000000	00000000	000060A5	000060B0
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	000060B8
Wininet.dll	1	00000000	00000000	00000000	000060B0	00006090

### Soluzione – Sezioni del malware

Da CFF Explorer, dalla sezione «section header» vediamo che l'eseguibile si compone di 3 sezioni. Purtroppo sembra che il malware abbia nascosto il vero nome delle sezioni e quindi non siamo in grado di capire che tipo di sezioni sono.

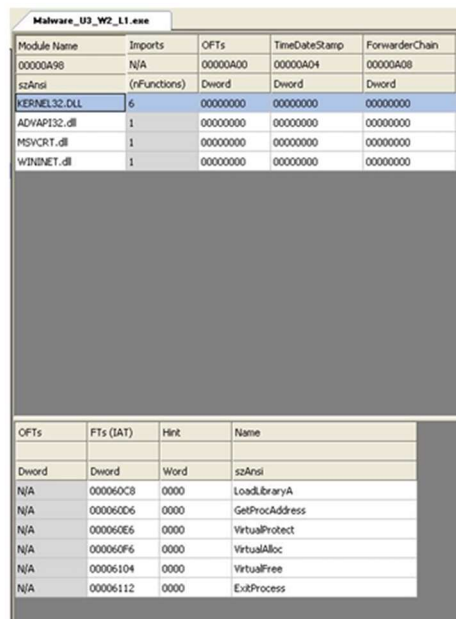


Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address
Byte[0]	Dword	Dword	Dword	Dword	Dword
LPX0	00004000	00001000	00000000	00000400	00000000
LPX1	00001000	00005000	00000600	00000400	00000000
LPX2	00001000	00006000	00000200	00000A00	00000000

### Soluzione – Considerazione finale

Si tratta di un malware avanzato che non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica.

Ciò è supportato dal fatto che tra le funzioni importate troviamo «**LoadLibrary** e **GetProcAddress**», che ci fanno pensare ad un malware che importa le librerie a tempo di esecuzione (runtime) nascondendo di fatto le informazioni circa le librerie importate a monte.

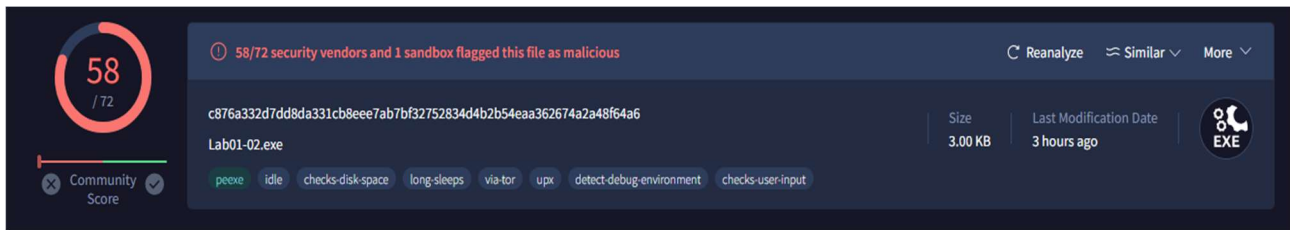


Module Name	Imports	OFIs	TimeDateStamp	ForwarderChain
00000A98	N/A	00000A00	00000A04	00000A08
szAnsi	(nFunctions)	Dword	Dword	Dword
Kernel32.dll	6	00000000	00000000	00000000
AdvAPI32.dll	1	00000000	00000000	00000000
MSVCRT.dll	1	00000000	00000000	00000000
Wininet.dll	1	00000000	00000000	00000000

OFIs	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

Inoltre se calcoliamo l'hash del file con **md5deep** e lo ricerchiamo su **VirusTotal** abbiamo conferma del fatto che è un malware.



The screenshot displays the VirusTotal analysis interface for a file named 'Lab01-02.exe'. On the left, a circular security score is shown as 58 out of 72, with a 'Community Score' indicator below it. A red banner at the top states '58/72 security vendors and 1 sandbox flagged this file as malicious'. The file's MD5 hash is 'c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6'. Metadata includes a size of 3.00 KB and a last modification date of 3 hours ago. The file type is identified as 'EXE'. A row of behavioral tags is visible: 'peexe', 'idle', 'checks-disk-space', 'long-sleeps', 'via-tor', 'upx', 'detect-debug-environment', and 'checks-user-input'. Action buttons for 'Reanalyze', 'Similar', and 'More' are located in the top right corner.

Property	Value
Security Score	58 / 72
File Name	Lab01-02.exe
MD5 Hash	c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Size	3.00 KB
Last Modification Date	3 hours ago
File Type	EXE
Behavioral Tags	peexe, idle, checks-disk-space, long-sleeps, via-tor, upx, detect-debug-environment, checks-user-input