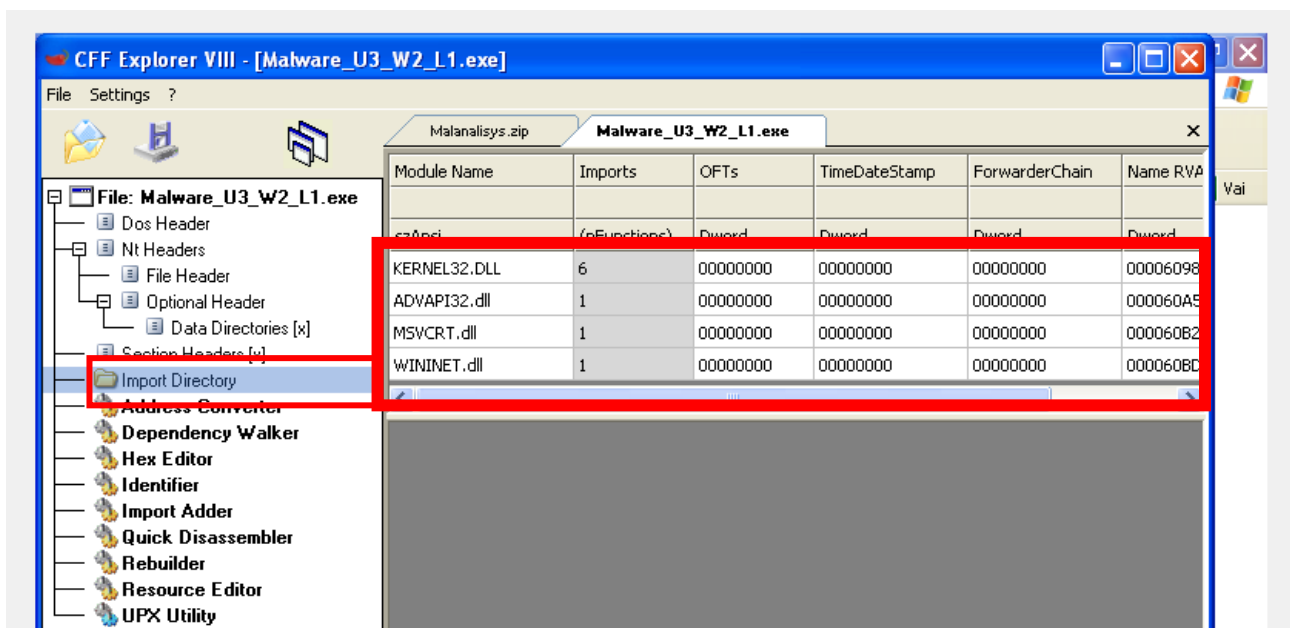


ANALISI STATICA BASICA

Ho aperto **CFF EXPLORER VIII**, selezionando la tab **IMPORT DIRECTORY** per vedere e librerie importate nel malware:

- **KERNEL32.DLL**: libreria usata per le funzioni principali per interagire con il sistema operativo. Un malware potrebbe sfruttare tale libreria per manipolare i file e per accedere la gestione della memoria
- **ADVAPI32.dll**: libreria che contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft, tramite la quale un malware potrebbe creare nuovi account utente, accedere al registro di sistema e crittografare o decrittografare dati sensibili;
- **MSVCRT.dll**: libreria che contiene funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output, come nel linguaggio C. Tramite questa libreria un malware potrebbe sfruttare delle vulnerabilità presenti o per eseguire codice malevolo;
- **WININET.dll**: libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP. Un malware potrebbe sfruttare tale libreria per comunicare con server remoti, scaricare e caricare file, inviare dati sensibili...



Selezionando la libreria KERNEL 32.DLL ho notato che al suo interno vi sono le funzioni **LoadLibraryA** e **GetProcAddress**, che permettono di importare le funzioni della libreria a **tempo di esecuzione (runtime)**. Ciò significa che l'eseguibile richiama la libreria solo quando ha bisogno di utilizzare una specifica funzione.

Questo è un comportamento tipico dei malware, i quali, attraverso questo meccanismo, cercano di risultare meno invasivi e rilevabili.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malanalysis.zip Malware_U3_W2_L1.exe

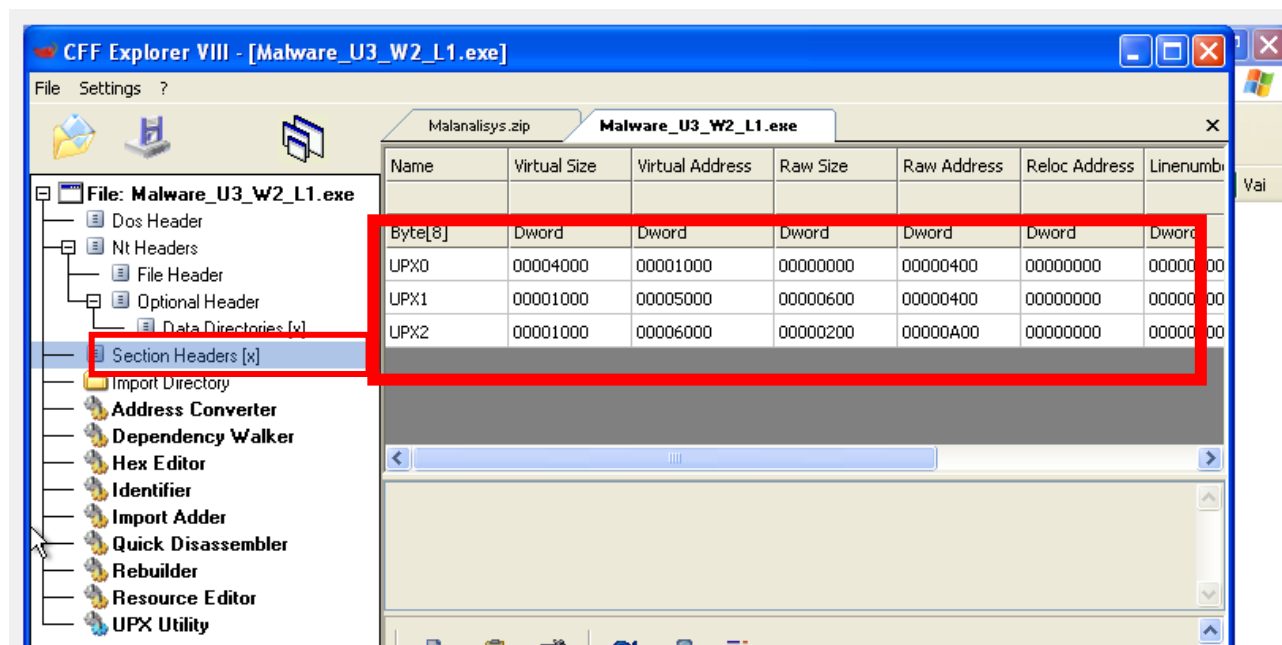
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5
MSVCRT.dll	1	00000000	00000000	00000000	000060B2
WININET.dll	1	00000000	00000000	00000000	000060BD

File: Malware_U3_W2_L1.exe

- Dos Header
- Nt Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

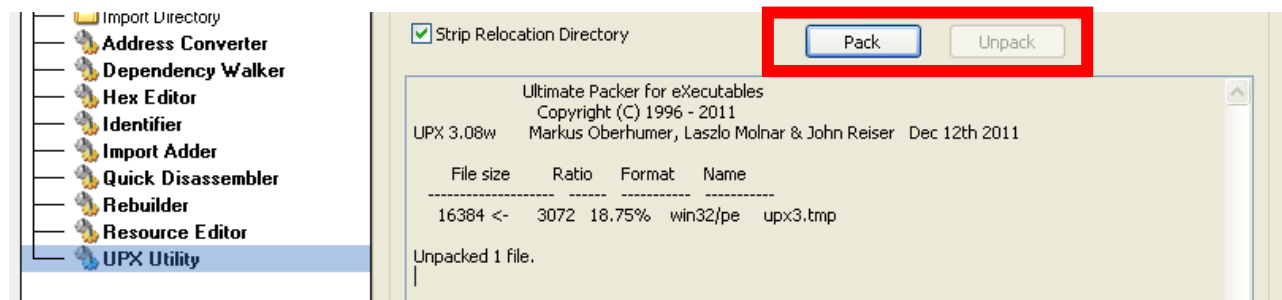
OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

In seguito ho selezionato la tab **SECTION HEADERS**, dove ho identificato le sezioni **UPX0**, **UPX1** e **UPX2**.



Adesso spostiamoci sulla sezione **UPX Utility**: procedendo all'estrazione con **"unpack"** abbiamo accesso alle seguenti sezioni:

- **.text**: Questa sezione contiene le istruzioni, ovvero le righe di codice che la CPU eseguirà quando il software viene avviato. È la sezione principale di un file eseguibile, poiché contiene il codice effettivo che viene eseguito per far funzionare il programma. Tutte le altre sezioni contengono dati o informazioni di supporto per questa sezione.
- **.rdata**: Questa sezione contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile. Qui vengono memorizzate le informazioni sui moduli esterni che l'eseguibile utilizza, come librerie di sistema o librerie condivise, e le funzioni che vengono importate o esportate per l'utilizzo all'interno del programma.
- **.data**: Questa sezione contiene dati e variabili globali del programma eseguibile. Le variabili definite in questa sezione sono accessibili da qualsiasi parte del programma, poiché sono globalmente dichiarate.



File: Malware_U3_W2_L1.exe	NAME	VIRTUAL SIZE	VIRTUAL ADDRESS	RAW SIZE	RAW ADDRESS	RAW ADDRESS	LINK NUMBER	RE
Dos Header	Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	W
Nt Headers	.text	000002DC	00001000	00001000	00001000	00000000	00000000	00
File Header	.rdata	00000372	00002000	00001000	00002000	00000000	00000000	00
Optional Header	.data	0000008C	00003000	00001000	00003000	00000000	00000000	00
Data Directories [x]								
Section Headers [x]								
Import Directory								

Ho scaricato md5deep su Windows XP, e tramite cmd ho preso l'hash del malware oggetto di interesse.

LINK DOWNLOAD: <https://sourceforge.net/projects/md5deep/files/md5deep/md5deep-4.3/>

```
C:\Documents and Settings\Epicode_user\Desktop\md5deep-4.3>md5deep.exe "C:\Documents and Settings\Epicode_user\Desktop\Malware_U3_W2_L1.exe"
8363436878404da0ae3e46991e355b83 C:\Documents and Settings\Epicode_user\Desktop\Malware_U3_W2_L1.exe
C:\Documents and Settings\Epicode_user\Desktop\md5deep-4.3>
```

Successivamente ho inserito su Virus Total l'hash ricavato grazie a MD5DEEP.



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

8363436878404da0ae3e46991e355b83

55
/ 70

55 security vendors and 1 sandbox flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Malware_U3_W2_L1.exe

Size: 3.00 KB
Last Analysis Date: 4 days ago

Reanalyze Similar More

peexe checks-disk-space via-tor detect-debug-environment idle long-sleeps upx checks-user-input

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 30+

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ulise/trojanclicker Threat categories trojan downloader Family labels ulise trojanclicker r002c0dhd20

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Generic.1ba980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Downloader.Gen

Risultato Virus Total: 53 vendors su 71 hanno identificato il malware come un tipo Trojan, comunicandoci per l'appunto la natura maligna del file oggetto di interesse.

Dai risultati delle analisi, possiamo trarre alcune conclusioni sul malware:

- Il malware è stato configurato **per utilizzare le connessioni di tipo HTTP/FTP/NTP** grazie all'importazione della libreria **Wininet.dll**. Questo suggerisce che **il malware potrebbe essere progettato per comunicare con server remoti, scaricare o caricare file o eseguire altre attività di rete utilizzando questi protocolli**.
- Il malware interagisce con il sistema operativo tramite la libreria **Kernel32.dll**. Questo indica che il malware utilizza funzioni di basso livello per accedere alle risorse del sistema, come la gestione dei file, la comunicazione con i processi e l'allocazione della memoria.
- L'analisi statica da sola non fornisce un quadro completo delle operazioni svolte dal malware. La presenza delle funzioni **LoadLibrary** e **GetProcAddress** **indica che il malware carica dinamicamente alcune funzioni durante l'esecuzione**. Pertanto, è necessaria un'analisi dinamica per ottenere ulteriori dettagli e osservare da vicino il comportamento del file.