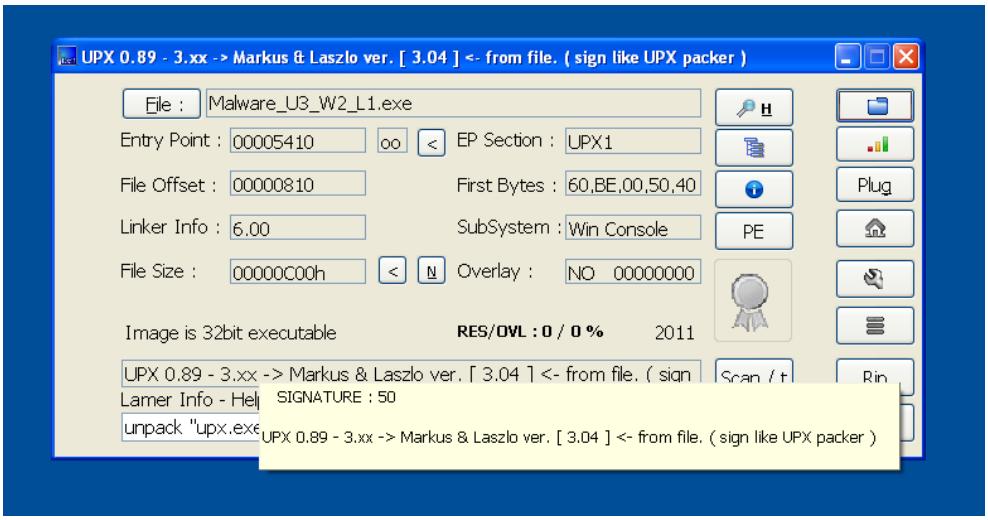
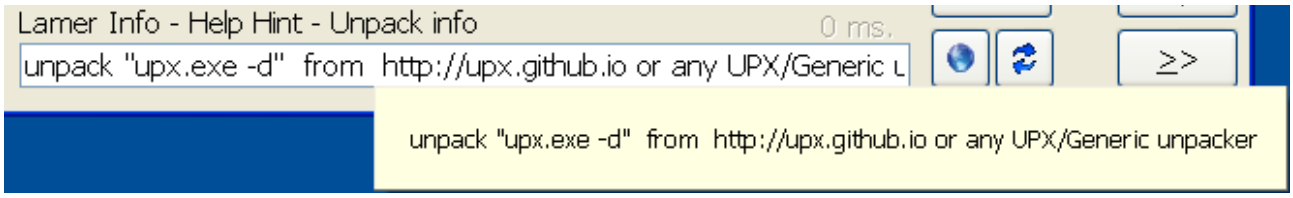
Report W10L1

VM: WinXp (Malware Analysis_Final)
Tools: ExeinfoPE-0.6.2; CFF Explorer-8.0; UPX-4.0.1; Pestudio-9.7.0

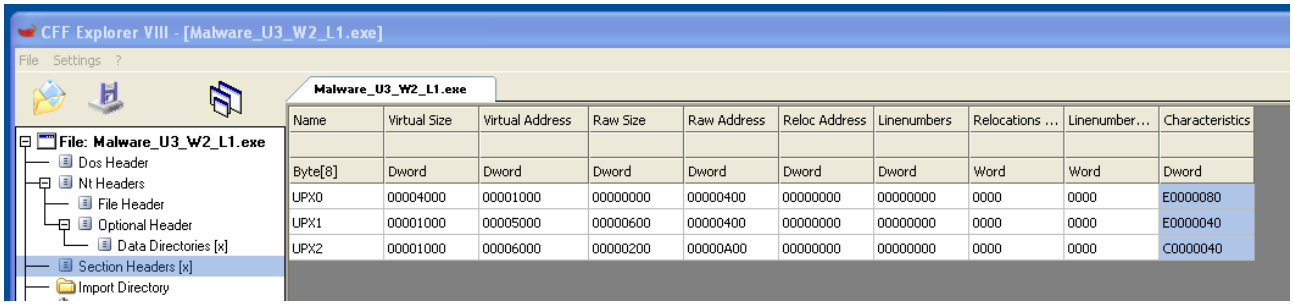
Indizio che il file sia packed:



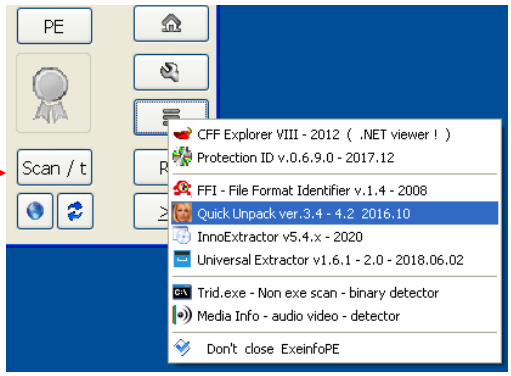
ExeinfoPE ci da anche informazioni da dove ottenere il unpacker:



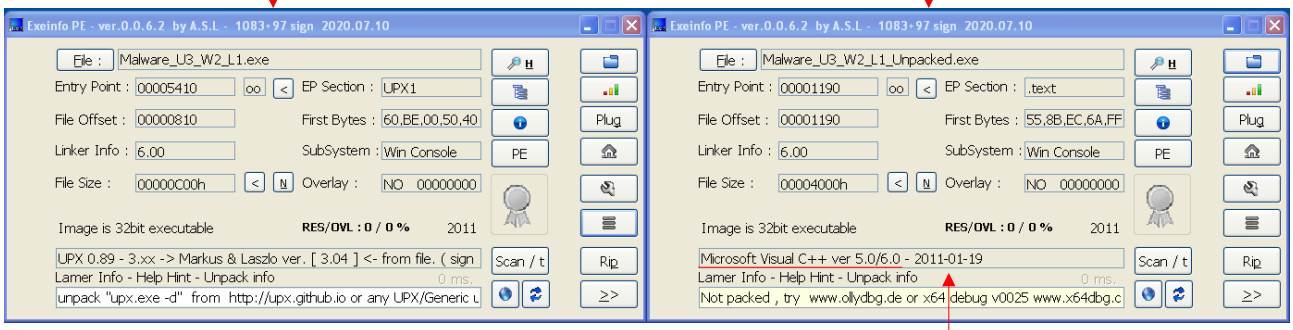
la prova usando CFF Explorer:
La prova sta nel Nome, UPX0, UPX1 ecc.



ExeinfoPE ci da la possibilità di fare “unpack” anche dalle proprie opzioni.

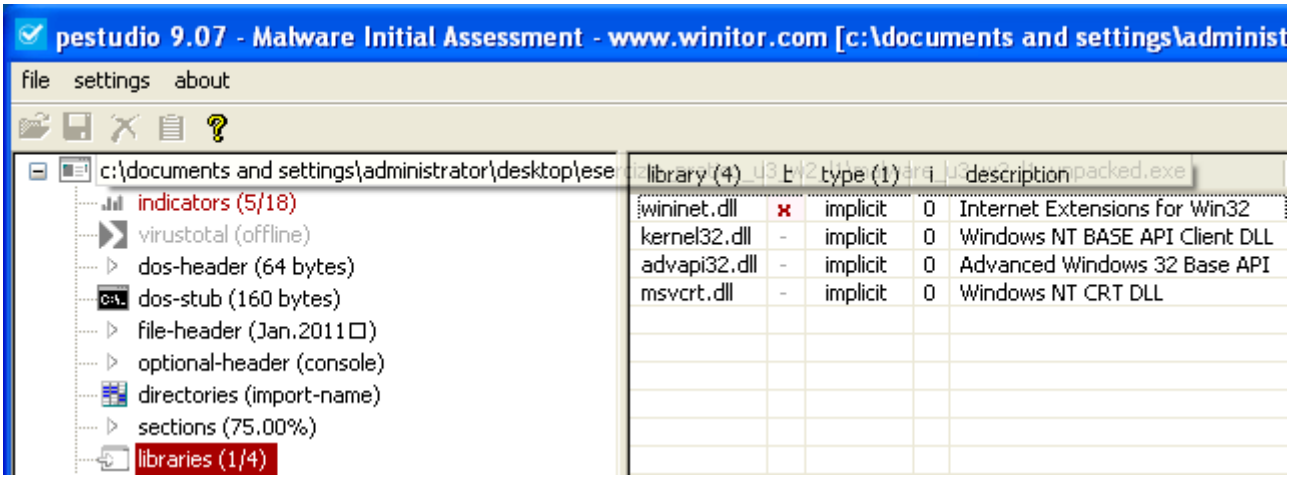


La differenza tra Packed e Unpacked



Le informazioni che possiamo notare sono molto utili, per esempio la data del “compiler-stamp” che ci può **suggerire** se il malware sia stato già analizzato e quindi renderci il lavoro più facile e il linguaggio del codice.

Proseguendo passeremo al PEstudio.

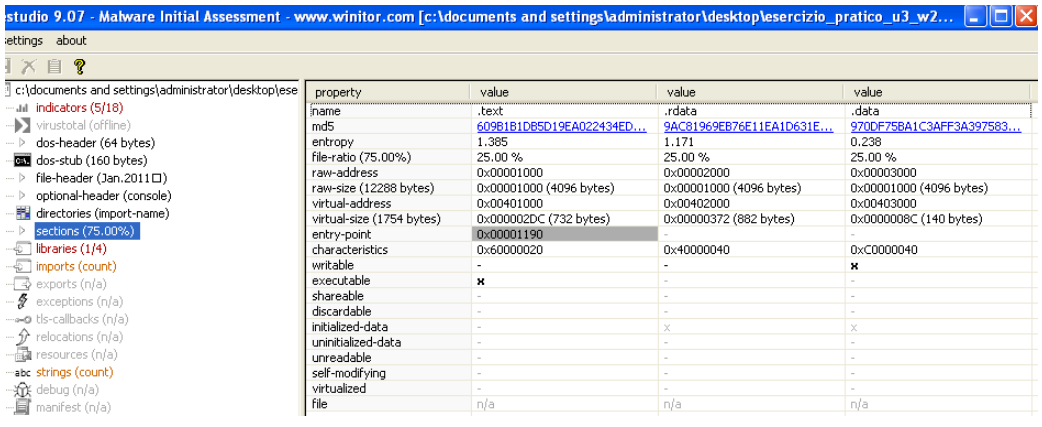


PEstudio ha la blacklist library integrata con le DLL(Dynamic Link Library) comunemente associate ai malware che sono utili per segnalarci dei flag che ci sia qualcosa di malintenzionato.

kernel32.dll lo troveremo quasi in tutte le .exe per quanto ci permette di interagire con il sistema
advapi32.dll è principalmente usato per modificare o interagire con il registry
msvcrt.dll è il componente del Microsoft Visual C Runtime Library
wininet.dll è usato per la socket connection e stabilire la connessione a internet

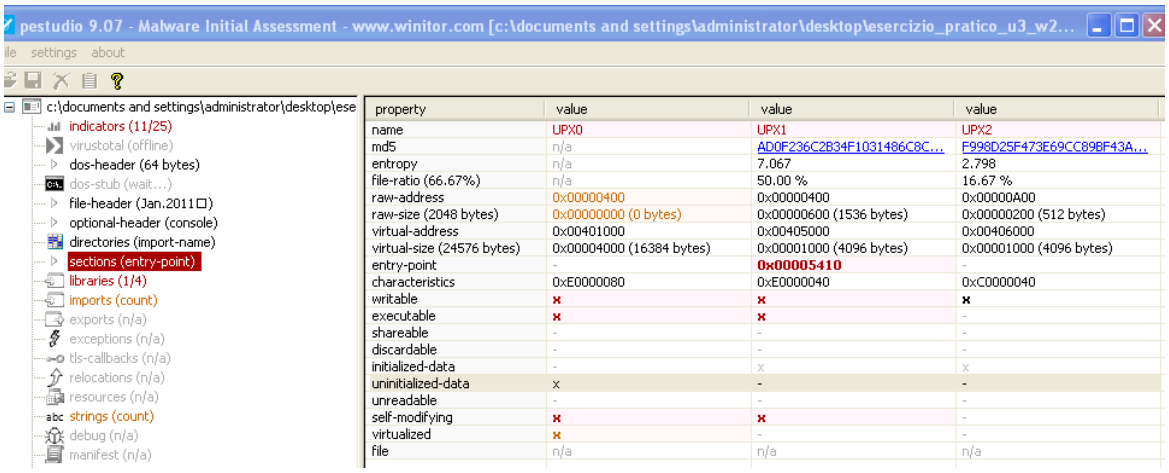
per maggiori informazioni PEstudio ci permette di fare la ricerca clicando sulla voce interessata con il tasto destro del mouse e cliccare sul search MSDN(MicroSoft Developer Network)

Unpacked:



Le sezioni contengono data e codice per l'executable (.exe)

.**text** è la sezioni che contiene il codice eseguibile
.**data** è la sezione che memorizza (stores) i data che possono essere Read e Write
.**rdata** è la sezione che memorizza (stores) il read-only data

Packed: 

property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	AD0F236C2B34F1031486C8C...	F998D25F473E69CC89BF43A...
entropy	n/a	7.067	2.798
file-ratio (66.67%)	n/a	50.00 %	16.67 %
raw-address	0x00000400	0x00000400	0x00000A00
raw-size (2048 bytes)	0x00000000 (0 bytes)	0x00000600 (1536 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00405000	0x00406000
virtual-size (24576 bytes)	0x00004000 (16384 bytes)	0x00001000 (4096 bytes)	0x00001000 (4096 bytes)
entry-point	-	**0x00005410**	-
characteristics	0xE0000080	0xE0000040	0xC0000040
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
unreadable	-	-	-
self-modifying	x	x	-
virtualized	x	-	-
file	n/a	n/a	n/a

Come possiamo notare, le sezioni UPX0 e UPX1 sono (writable, executable e self-modifying) che suggerisce che il malware è composto in queste 2 sezioni.

type (2)	size (bytes)	file-offset	blacklist (5)	hint (6)	value (56)
ascii	17	0x000021B7	x	-	GetModuleFileName
ascii	13	0x0000223F	x	-	CreateService
ascii	26	0x0000224F	x	-	StartServiceCtrlDispatcher
ascii	15	0x0000232D	x	-	InternetOpenUrl
ascii	12	0x0000233F	x	-	InternetOpen
ascii	34	0x00003030	-	url-pattern	http://www.malwareanalysisbook.com
ascii	12	0x0000216C	-	file	KERNEL32.DLL
ascii	12	0x00002179	-	file	ADVAPI32.dll
ascii	10	0x00002186	-	file	MSVCRT.dll
ascii	11	0x00002191	-	file	WININET.dll
ascii	40	0x0000004D	-	dos-message	!This program cannot be run in DOS mode.

GetModuleFileName = Questa funzione restituisce il nome file di un modulo caricato nel processo corrente. Il malware può utilizzare questa funzione per modificare o copiare i file nel processo attualmente in esecuzione.
CreateService = Questa funzione viene utilizzata per creare un servizio che può essere avviato al momento dell'avvio. Il malware utilizza CreateService per la persistenza, l'occultamento o per caricare i driver del kernel.
StartServiceCtrlDispatcher = Questa funzione viene utilizzata da un servizio per connettere il thread principale del processo al gestore di controllo del servizio. Qualsiasi processo eseguito come servizio deve chiamare questa funzione entro 30 secondi dall'avvio. L'individuazione di questa funzione nel malware indicherà che la funzione deve essere eseguita come servizio.
InternetOpenURL = Questa funzione apre un URL specifico per una connessione tramite FTP, HTTP o HTTPS. Gli URL, se corretti, spesso possono essere buone firme basate sulla rete.
InternetOpen = Questa funzione inizializza le funzioni di accesso a Internet di alto livello da WinINet, come InternetOpenUrl e InternetReadFile. La ricerca di InternetOpen è un buon modo per trovare l'inizio della funzionalità di accesso a Internet. Uno dei parametri di InternetOpen è lo User-Agent, che a volte può creare una buona firma basata sulla rete.