

ANALISI STATICA BASICA

TASK

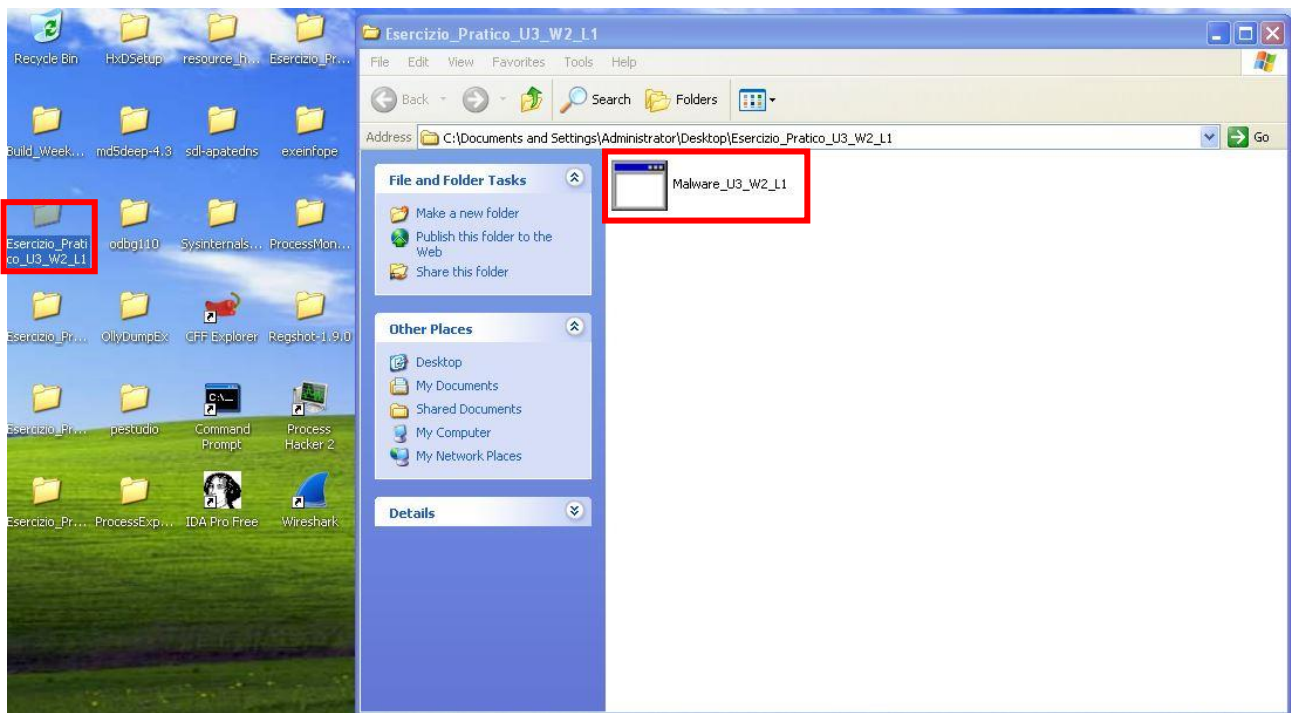
Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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

ANALISI E VALUTAZIONI

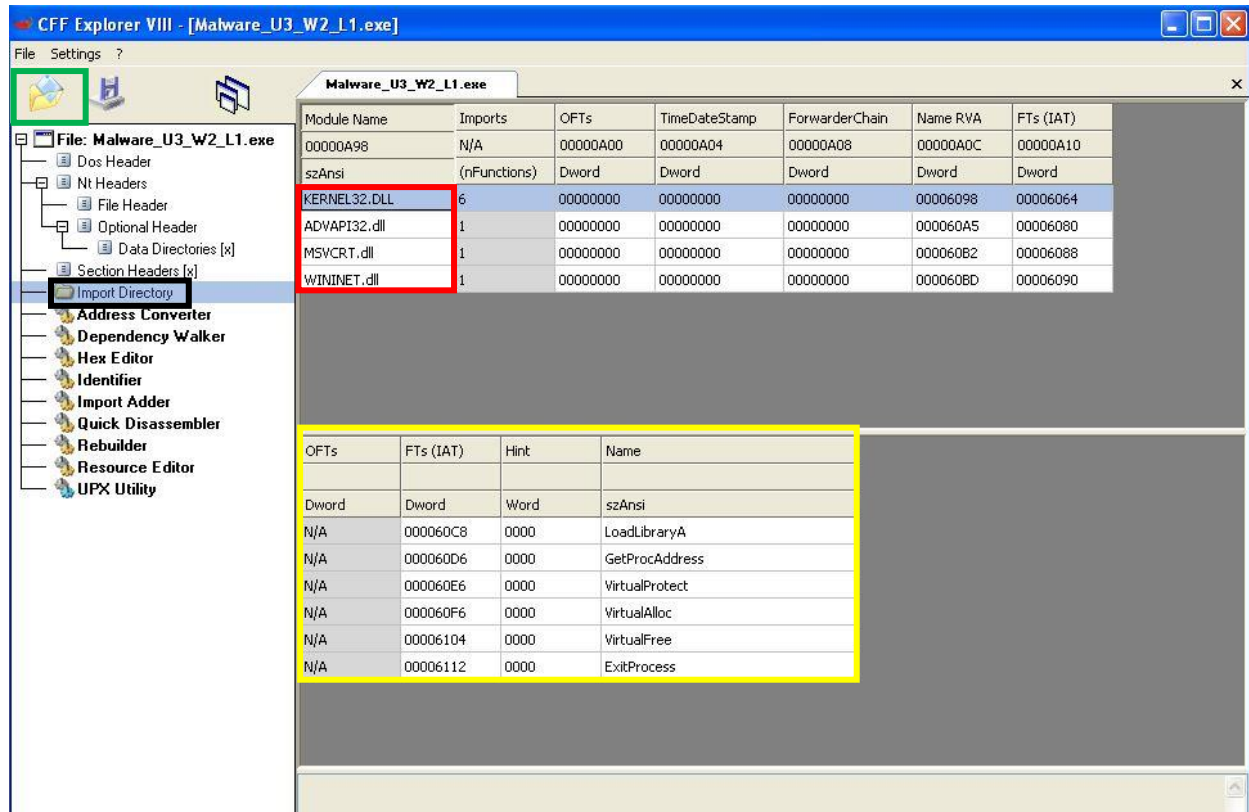
Come prima cosa andiamo a prendere il nostro file in esame nella cartella dal nome <<**Esercizio_Pratico_U3_W2_L1**>> che si troverà sul desktop:



Come passo successivo andiamo ad analizzare il file utilizzando i tool visti nella lezione teoria come: **CFF Explorer** e **Exeinfo PE**.

LIBRERIE IMPORTATE DAL MALWARE

Per andare a scovare le librerie importate dal malware utilizziamo il tool **CFF Explorer** che avremo da desktop. All'apertura, e caricando il file, andiamo nella sezione a sinistra denominata **Import Directory**. Da qui possiamo vedere le librerie che sono state importate:



LEGGENDA:

- ☐ Permette di caricare il file
- ☐ Sezione di analisi
- ☐ Permette di visualizzare a schermo le librerie importate
- ☐ Permette di visualizzare a schermo le funzioni della libreria selezionata

Andiamo ora ad analizzare le librerie ottenute, abbiamo:

- **KERNEL32.DLL** = Libreria che contiene le funzioni principali per interagire con il sistema operativo. Es. gestione della memoria, manipolazione del file.
- **ADVAPI32.dll** = Libreria che contiene le funzioni per interagire con i servizi e i registri del sistema operativo Microsoft.
- **MSVCRT.dll** = Libreria che contiene funzioni per la manipolazione di stringhe, allocazione di memoria e altro come chiamate input/output.
- **WININET.dll** = Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Mentre le funzioni ricavate sono in totale 9, di cui:

- 6 x Kernell32.dll
- 1 x Advapi32.dll
- 1 x Msvcrt.dll
- 1 x Wininet.dll

N/A	00006120	0000	CreateServiceA
N/A	00006130	0000	exit
N/A	00006136	0000	InternetOpenA

SEZIONI DI CUI SI COMPONE IL MALWARE

In **CFF** basterà andare nella sezione denominata **Section Headers** e tra i risultati ottenuti abbiamo:

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File: **Malware_U3_W2_L1.exe**

Section Headers:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Cha
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E00
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E00
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C00

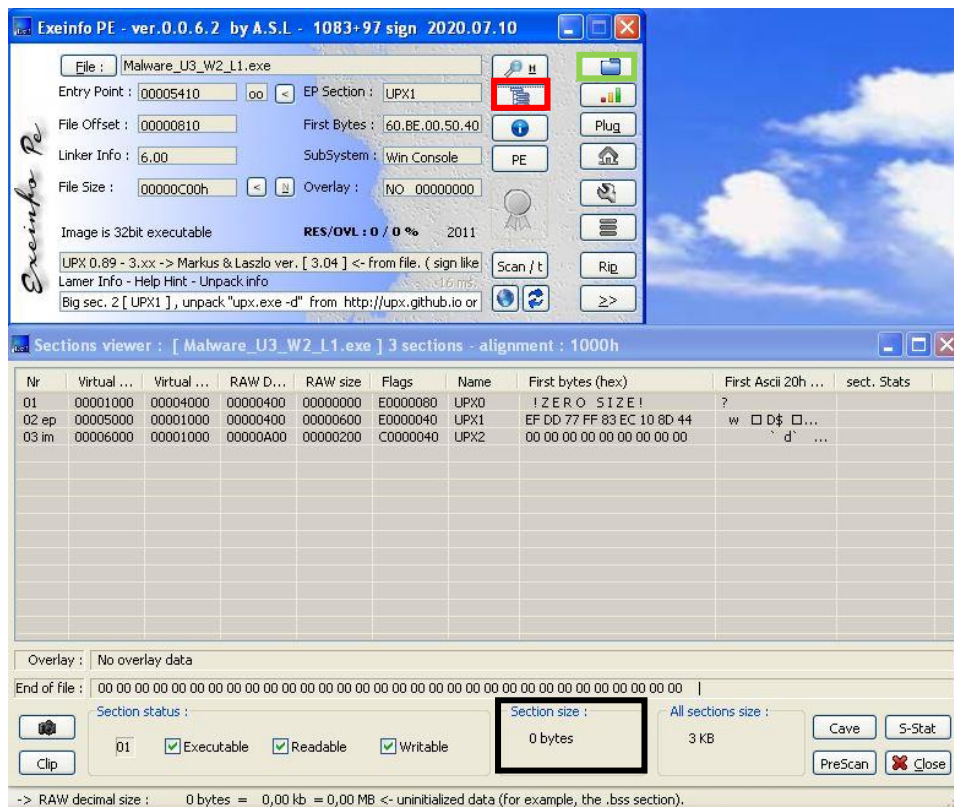
This section contains:

Code Entry Point: 00005410
Data: 00006000
Import Directory: 00006000

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	EF	DD	77	FF	83	EC	10	8D	44	24	00	C7	03	10	30	40	iYwYi111Ds.C110@
00000010	00	50	08	08	40	10	40	10	B7	FD	E9	DC	0C	00	00	07	.F11@1.ýéÜ111
00000020	10	FF	15	04	20	15	6A	01	BD	FD	FE	5D	E8	0D	3C	83	1Y111j1ýü1ë.<1
00000030	C4	18	C3	90	00	81	EC	00	04	0F	68	28	30	E9	BE	E9	ÄÄÄ1111h(0é1é
00000040	FE	1C	68	01	00	1F	29	20	85	C0	74	08	6A	0B	1C	67	bth1111ÄÄ1j11lg
00000050	DF	17	AC	56	1E	0F	2C	45	03	0B	08	F6	6D	EF	36	8B	B1-V1111E111ömi61
00000060	F0	7E	1C	68	E8	03	44	50	13	14	65	76	B7	FD	0B	01	8~1hè1DP11ev.ý11
00000070	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	6C	63	EE	68	1Is.1Q.1j11Ülc1h

Da cui si ottengono le seguenti sezioni, le quali sono compresse sotto forma **UPX** un software in grado di comprimere le sezioni:

- **UPX0** = Unione di UPX1 e UPX2 di fatti se andassimo a prendere la descrizione nel rettangolo sotto (blu in figura soprastante) questo ci permette di intuire, dopo aver analizzato anche le altre due sezioni, che è l'unione di UPX1 e UPX2. E che pertanto possiamo definirlo come una sezione di tipo .text contenente le istruzioni e le righe di codice che la CPU eseguirà una volta che il software verrà avviato. Si può notare un'altra particolarità, che se andando ad analizzare la stessa sezione presa in esame, sull'altro tool (Exeinfo PE) la grandezza è di circa 0 bytes, idoneo per un file.txt



Per arrivare a questa sezione andiamo a caricare dapprima il file (riquadro verde), successivamente apriamo il file dall'icona (riquadro rosso) e infine notiamo questa particolarità della grandezza, dopo aver selezionato il nostro UPX0, dal riquadro nero in figura soprastante.

- **UPX1** = Possiamo paragonarlo ad **.data** ovvero che contiene al suo interno tipicamente i dati/variabili del programma eseguibile. Come si può vedere dall'ASCI della foto successiva:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	EF	DD	77	FF	83	EC	10	8D	44	24	00	C7	03	10	30	40	iYwY111D\$.C110@
00000010	00	50	08	08	40	10	40	10	B7	ED	E9	DC	0C	00	00	07	P110101.yeU...
00000020	10	FF	15	04	20	15	6A	01	B0	FD	E9	5D	E8	0D	3C	93	1111111111111111
00000030	C4	18	C3	90	00	81	EC	00	04	0F	68	28	30	E9	BE	E9	A111111111111111
00000040	FE	1C	68	01	00	1F	29	20	85	C0	74	08	6A	0B	1C	67	b111111111111111
00000050	DF	17	AC	56	1E	0F	2C	45	03	0B	08	F6	D	EF	36	8B	B1-V11111111111111
00000060	F0	7E	1C	68	E8	03	44	50	13	14	65	76	B7	FD	0B	01	8~the1DP1111111111
00000070	8D	4C	24	2C	05	51	0A	02	6A	10	03	D9	6C	63	EE	68	ILS,1Q,111111111111
00000080	1C	45	04	56	3B	00	33	D2	66	B7	EB	BE	14	89	54	24	IEIV:30f:ek11111111
00000090	04	29	04	07	08	50	04	10	51	6C	49	B6	DF	18	66	C0	1111111111111111
000000A0	34	08	50	10	0B	18	CB	AD	6D	93	8D	22	20	7A	15	52	4111111111111111
000000B0	56	24	EB	3F	D6	3D	FF	08	28	E7	75	2B	57	8B	3D	30	V8s70=y1(-u-W1=0
000000C0	0A	BE	14	FF	C1	3E	73	E9	2E	68	50	11	C0	D7	4E	75	.%1vA)se hP1A1Nu
000000D0	EC	5F	33	C0	5E	EC	D9	65	DF	81	C4	F7	C3	09	90	00	i_3A11111111111111
000000E0	56	57	BD	B1	CF	E6	1E	01	68	54	A9	E4	74	3D	70	EA	VWkt11111111111111
000000F0	7D	6C	AD	C7	48	52	80	51	30	C7	D7	EB	EB	90	65	F7	11-sHR100Cxe1e1e+
00000100	F6	84	00	55	8B	EC	8B	68	80	20	E9	D0	12	ED	C2	FB	ol_U11111111111111
00000110	C3	64	A1	7C	50	64	89	25	07	AC	20	53	60	DE	9B	CD	Ad1Pd111111111111
00000120	FD	89	65	E8	83	65	FC	61	5C	60	59	83	0D	80	69	EB	yleeteua\Y11111111
00000130	7E	DB	D9	06	84	14	5C	6B	0D	7C	0C	89	FF	77	64		~0U11111111111111
00000140	AC	58	0D	78	A1	54	0C	00	A3	88	0D	E6	EB	FB	06	C6	-X x11111111111111
00000150	02	BD	83	3D	6C	0A	00	75	0C	68	BE	6C	4F	C1	1E	FE	1111111111111111
00000160	CE	50	19	A8	68	0C	6C	08	28	37	F7	ED	EF	A2	A1	74	IP1111111111111111
00000170	40	45	D8	8D	02	50	FF	35	70	0C	09	E0	50	BE	EF	D6	@E1111111111111111
00000180	6C	03	D4	E4	11	15	48	B0	04	32	00	B6	FB	6D	43	14	110a111111111111
00000190	44	6D	4D	E0	85	75	E0	02	6D	1B	ED	CB	D4	E4	E8	8D	DmMatua1111111111
000001A0	FD	A0	3B	30	49	DC	FD	F7	FF	D7	34	40	1F	45	EC	8B	y_01Uy+yx4@111111
000001B0	08	8B	09	89	4D	D0	50	51	36	9C	59	59	C3	8B	C6	6E	1111111111111111
000001C0	B6	AD	E0	2B	D0	1F	38	FF	25	3C	05	4C	F3	35	DE	F6	1111111111111111
000001D0	60	1F	03	04	65	29	D2	B2	25	EC	05	7E	C3	C3	CC	00	1111111111111111
000001E0	2F	64	80	28	32	33	68	00	00	37	A0	39	FF	80	7B	94	/d1(23h_7_9y111111
000001F0	12	B2	04	44	91	AF	0B	29	FF	8F	8A	4D	61	6C	53	65	1111111111111111
00000200	72	76	69	63	65	FE	DB	3F	A4	73	48	47	4C	33	34	35	rv1cep07sHGL345
00000210	07	68	74	74	70	3A	2F	2F	77	FF	B7	BF	DD	00	2E	6D	11http://wy-1Y..m
00000220	1E	77	61	72	65	61	6E	07	79	73	69	73	62	6F	6F	6B	11varean111111111111
00000230	2E	63	6F	FF	DB	DB	6F	6D	23	49	6E	74	36	6E	65	74	.coy00om1111111111
00000240	20	45	78	70	6C	6F	21	72	20	38	46	45	49	C7	2E	30	Exp101r:8FE1C,0
00000250	3C	01	20	01	A0	C0	09	65	73	14	15	98	10	10	EF	3D	1111111111111111
00000260	FF	FF	01	53	79	73	74	65	6D	54	69	6D	65	54	6F	46	yy11SystemTime1of
00000270	69	6C	65	15	47	65	74	4D	6F	C1	B6	FC	DA	64	75	0E	1111GetMod1111111111
00000280	12	4E	61	41	13	43	76	67	7F	2B	F3	2A	57	61	69	74	11Na1Cvg1111111111
00000290	61	62	27	72	15	45	78	B7	FD	ED	DF	0F	50	72	6F	63	ab'rtEx-y1111111111

- **UPX2** = Quest'ultimo invece può essere interpretato come un **.rdata** in quanto ci sono scritte sia le librerie importate che le loro funzioni. Come si evince dall'ASCII nell'immagine successiva:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	98	60	00	00	00	d.....
00000010	64	60	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	A5	60	00	00	80	60	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	B2	60	00	00	88	60	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	BD	60	00	00	90	60	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	C8	60	00	00	D6	60	00	00	E6	60	00	00
00000070	F6	60	00	00	04	61	00	00	12	61	00	00	00	00	00	00
00000080	20	61	00	00	00	00	00	00	30	61	00	00	00	00	00	00
00000090	36	61	00	00	00	00	00	00	4B	45	52	4E	45	4C	33	32	6a.....
000000A0	2E	44	4C	4C	00	41	44	56	41	50	49	33	32	2E	64	6C	.DLL.ADVAPI32.dl
000000B0	6C	00	4D	53	56	43	52	54	2E	64	6C	6C	00	57	49	4E	l.MSVCRT.dll.WIN
000000C0	49	4E	45	54	2E	64	6C	6C	00	4C	6F	61	64	4C	69	00	INET.dll..LoadLi
000000D0	62	72	61	72	79	41	00	00	47	65	74	50	72	6F	63	41	braryA..GetProcA
000000E0	64	64	72	65	73	73	00	00	56	69	72	74	75	61	6C	50	ddress..VirtualP
000000F0	72	6F	74	65	63	74	00	00	56	69	72	74	75	61	6C	41	rotect..VirtualA
00000100	6C	6C	6F	63	00	00	56	69	72	74	75	61	6C	46	72	65	lloc..VirtualFre
00000110	65	00	00	00	45	78	69	74	50	72	6F	63	65	73	73	00	e...ExitProcess.
00000120	00	00	43	72	65	61	74	65	53	65	72	76	69	63	65	41	..CreateServiceA
00000130	00	00	65	78	69	74	00	00	49	6E	74	65	72	6E	65	74	..exit..Internet
00000140	4F	70	65	6E	41	00	00	00	00	00	00	00	00	00	00	00	OpenA..Internet
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

CONSIDERAZIONE FINALE SUL MALWARE

Possiamo dunque dire in conclusione che attraverso le informazioni ottenute da librerie, funzioni e sezioni, il malware analizzato in questione:

- Funzione Wininet.dll: all'interno della libreria si ha una funzione denominata **InternetOpenA** la quale si presuppone che il malware avvi la connessione con protocolli di tipo HTTP, FTP o NTP.
- Funzione Advapi.dll: al suo interno ritroviamo la funzione **CreateServiceA** e si presuppone che il malware crei un oggetto sulla macchina vittima.
- Libreria Kernell.dll: al suo interno ritroviamo diverse funzioni che ipotizziamo permettano all'attaccante di interagire con il sistema operativo.

Il tutto però è una supposizione in quanto il malware è compresso con software UPX il che non permette di visualizzare totalmente le funzioni delle librerie prese in esame.