

S10L1

Rosario Z.

Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi dinamica basica. Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L2» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- **Identificare eventuali azioni del malware sul file system utilizzando Process Monitor**
- **Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor**
- **Provare a profilare il malware in base alla correlazione tra «operation» e Path.**

Suggerimento: Per quanto riguarda le attività del malware sul file system, soffermatevi con particolare interesse sulle chiamate alla funzione Create File su path noti (ad esempio il path dove è presente l'eseguibile del malware).

TRACCIA 1

- Identificare eventuali azioni del malware sul file system utilizzando Process Monitor

Per analizzare il file sospetto utilizziamo un tool già presente sulla macchina virtuale Con sistema operativo Windows XP fornito.

La figura 1 ci mostra alcuni dettagli interessanti fra la quale le dimensioni, che risultano ridotte, questo ci fa pensare a semplice e poco pesante codice malevolo.

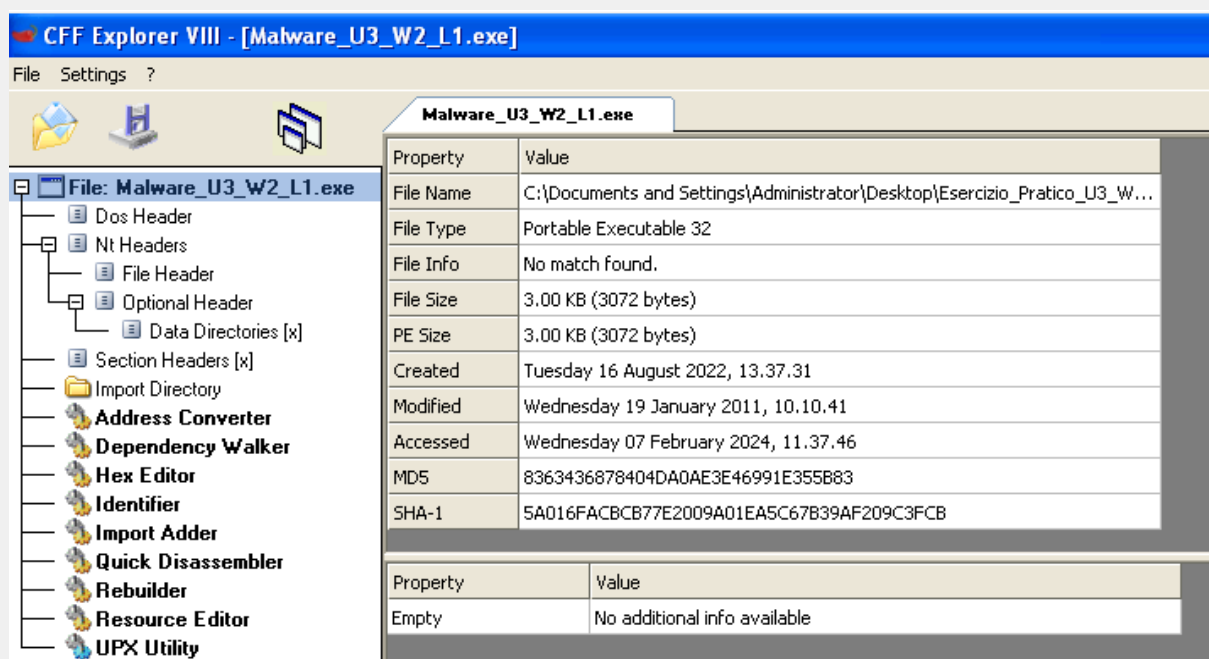
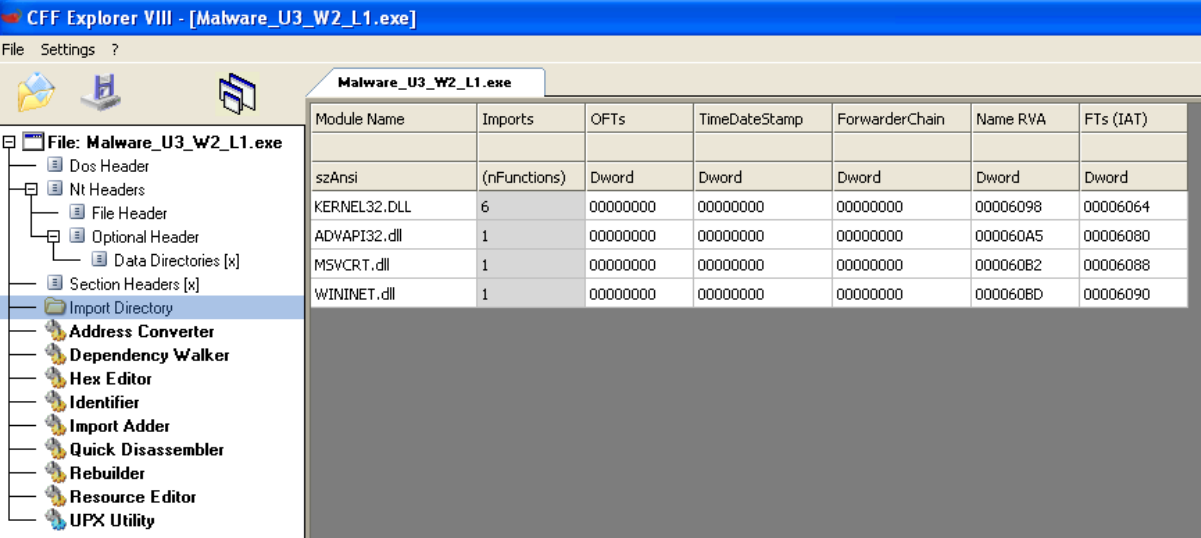


Figura 1

Dirigendoci sulla cartella “Import Directory” possiamo osservare invece quali cartelle il Malware va ad utilizzare. La Figura 2 ci mostra l’utilizzo da parte del malware della directory “kernel.32.dll”, come anche l’utilizzo di altre cartelle sensibili.



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

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

Figura 2

Traccia 2

- Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

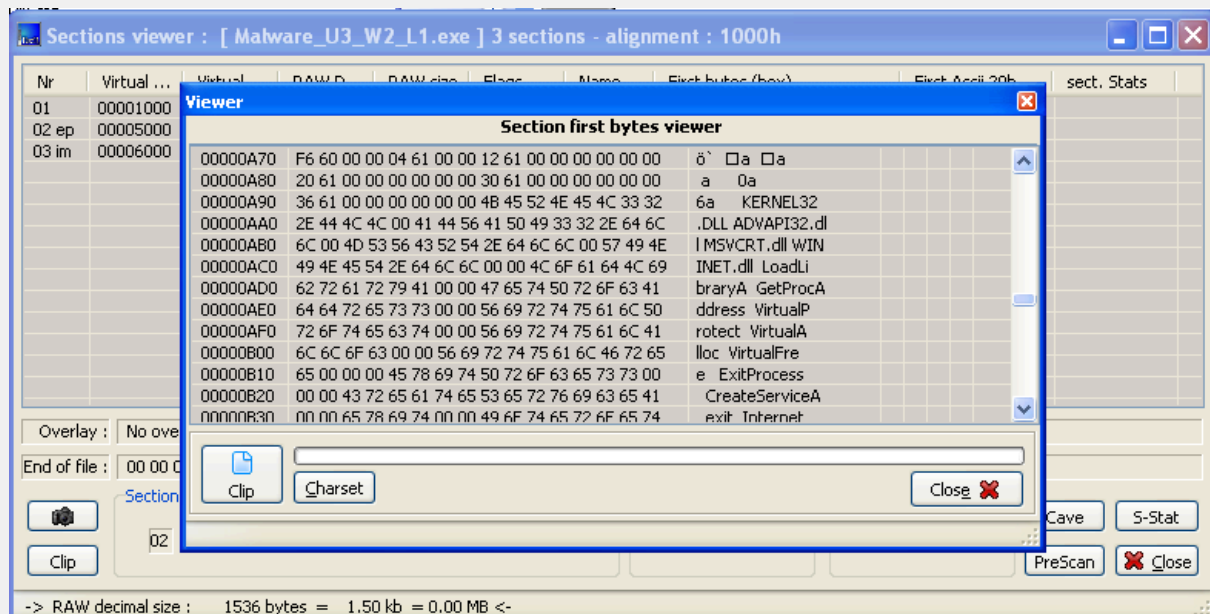
Come possiamo notare: Il codice ASCII presenta delle anomalie (Figura 3)

The screenshot shows the CFF Explorer VIII interface for the file **Malware_U3_W2_L1.exe**. The left sidebar displays the file structure, with **Section Headers [x]** selected. The main pane shows a table of section headers:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	C0000040

Below the section headers, the **UPX Utility** section is expanded, showing a hex dump of the ASCII section. The hex dump displays the raw data of the section, with the ASCII column showing the corresponding text. The text is a mix of valid ASCII characters and non-printable bytes (00), indicating anomalies in the code.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZi...yy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	0E	1F	EA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	!!...I...LITh
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t.be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$
00000080	E3	C1	65	8F	A7	A0	0B	DC	A7	A0	0B	DC	A7	A0	0B	DC	aa\$ iUS iUS iU
00000090	4F	BF	01	DC	AC	A0	0B	DC	24	BC	05	DC	A6	A0	0B	DC	00 iU~ iUS iU iU
000000A0	4F	BF	0F	DC	A5	A0	0B	DC	A7	A0	0B	DC	A3	A0	0B	DC	00 iU~ iUS iU iU
000000B0	A7	A0	0A	DC	BC	A0	0B	DC	C5	BF	18	DC	A2	A0	0B	DC	\$ U4 iU&iUo iU
000000C0	4F	BF	00	DC	A5	A0	0B	DC	52	69	63	68	A7	A0	0B	DC	00 iU# iURich\$ iU
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	50	45	00	00	4C	01	03	00	01	0D	37	4D	00	00	00	00	PE...L...7M...
000000F0	00	00	00	00	E0	00	0F	01	0B	01	06	00	00	10	00	00a.....P...
00000100	00	10	00	00	00	40	00	00	10	54	00	00	00	50	00	00@...T...P...



Come possiamo notare il Malware crea dei processi e servizi

Traccia 3

- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

Il malware è avanzato e non ci consente di recuperare molte informazioni sul suo comportamento con l'analisi statica basica.

