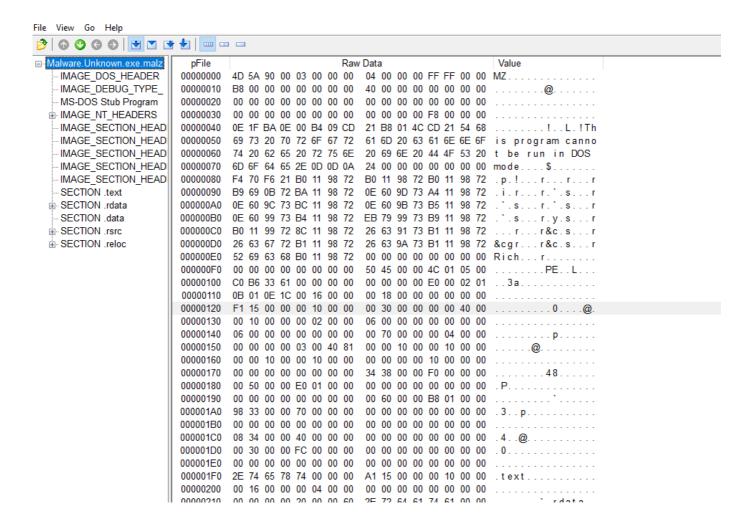
## **Analyzing the import Address Table (PE View)**

## **Analyzing the import Address Table (PE View)**

PE: Portable Executable

It is nothing more than a gigantic array of bytes, which will be our Malware

In PE view you can see Pfile(Address) ,Raw Data , Actual value.



This **MZ** The two starting byte will give you the idea what this file is.

IMAGE\_FILE\_HEADER under Image section will have the **time stamp** which can be correct or incorrect.

The malwares compiled with Borland Delphi Compiler Will always have a timestamp of 1992

■ Malware.Unknown.exe.malz	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000000FC	014C	Machine	IMAGE_FILE_MACHINE_I386
IMAGE_DEBUG_TYPE_	000000FE	0005	Number of Sections	
MS-DOS Stub Program	00000100	6133B6C0	Time Date Stamp	2021/09/04 Sat 18:11:12 UTC
image_nt_headers	00000104	00000000	Pointer to Symbol Table	
Signature	00000108	00000000	Number of Symbols	
··· IMAGE_FILE_HEADEI	0000010C	00E0	Size of Optional Header	
IMAGE_OPTIONAL_H	0000010E	0102	Characteristics	
IMAGE_SECTION_HEAD			0002	IMAGE_FILE_EXECUTABLE_IMAGE
IMAGE_SECTION_HEAD			0100	IMAGE_FILE_32BIT_MACHINE
IMAGE_SECTION_HEAD				
IMAGE_SECTION_HEAD				

Now, Take a good look at <code>IMAGE\_FILE\_HEADER .text</code> Here we can see the **virtual size** and **size of raw data**, it will be in Hex, So use a calculator to compare their size

If Virtual size is > Size of raw data then we may be dealing with a packed binary.

	pFile	Data	Description	Value
IMAGE_DOS_HEADER	000001F0	2E 74 65 78	Name	.text
IMAGE_DEBUG_TYPE_	000001F4	74 00 00 00		
MS-DOS Stub Program	000001F8	000015A1	Virtual Size	
□ IMAGE_NT_HEADERS	000001FC	00001000	RVA	
Signature	00000200	00001600	Size of Raw Data	
··· IMAGE_FILE_HEADER	00000204	00000400	Pointer to Raw Data	
IMAGE_OPTIONAL_HEADER	00000208	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER .text	0000020C	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER .rdata	00000210	0000	Number of Relocations	
IMAGE_SECTION_HEADER .data	00000212	0000	Number of Line Numbers	
IMAGE_SECTION_HEADER .rsrc	00000214	60000020	Characteristics	
IMAGE_SECTION_HEADER .reloc			00000020	IMAGE_SCN_CNT_CODE
SECTION .text			20000000	IMAGE_SCN_MEM_EXECUTE
⇒ SECTION .rdata			40000000	IMAGE_SCN_MEM_READ
IMPORT Address Table				
IMAGE_DEBUG_DIRECTORY				
IMAGE_LOAD_CONFIG_DIRECTORY				
- IMAGE DEBUG TYPE CODEVIEW				
IMAGE DEBUG TYPE				

One of the Important Info We can get in <code>IMPORT Address Table</code> Under <code>SECTION .rdata</code> To Understand this we have to understand <code>Windows API</code> .

- Dont forgot procmon,procwatch,proc explore (John.H)
- always open three of them for use
- regshot learn about about
  - To caputure wht registry changed and can compare
- · cscript.exe run .js file in cmd