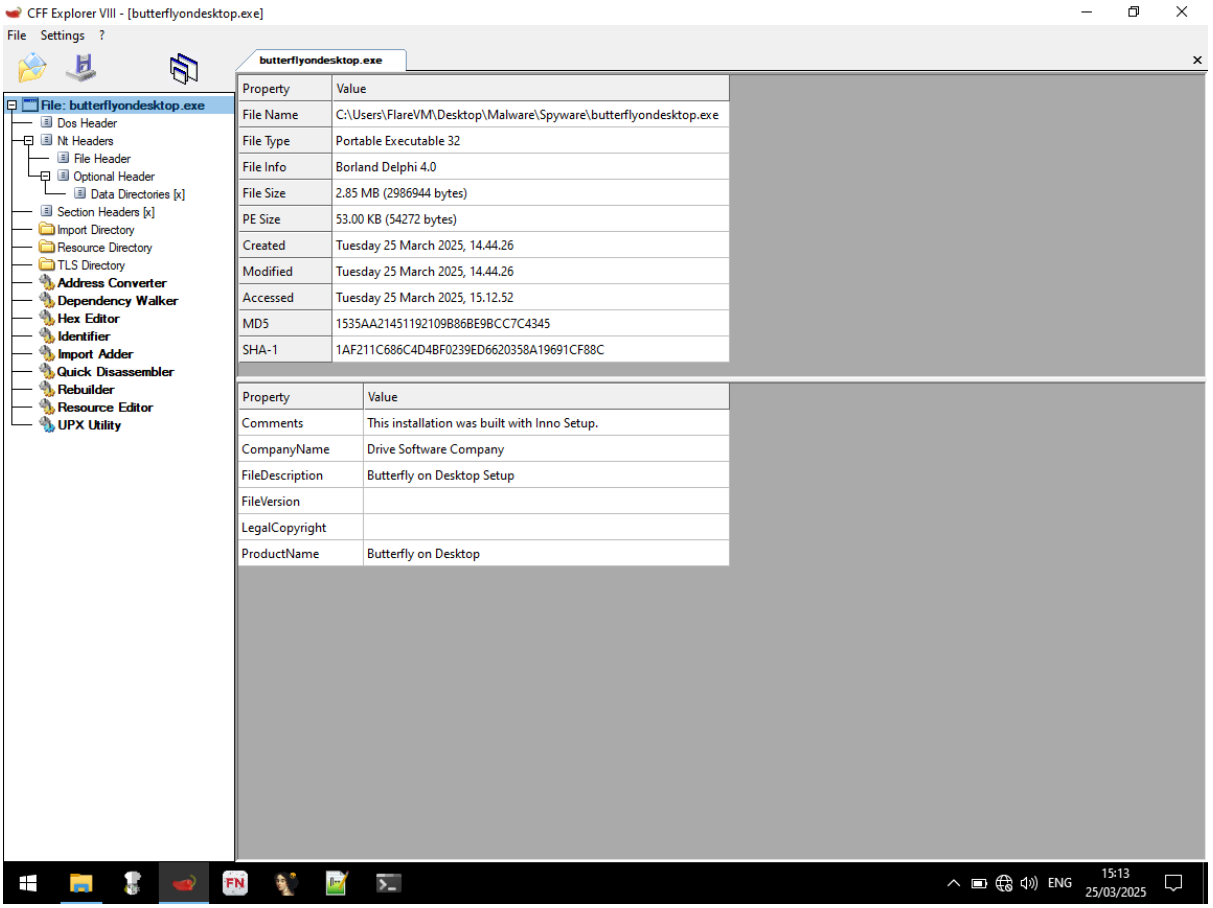
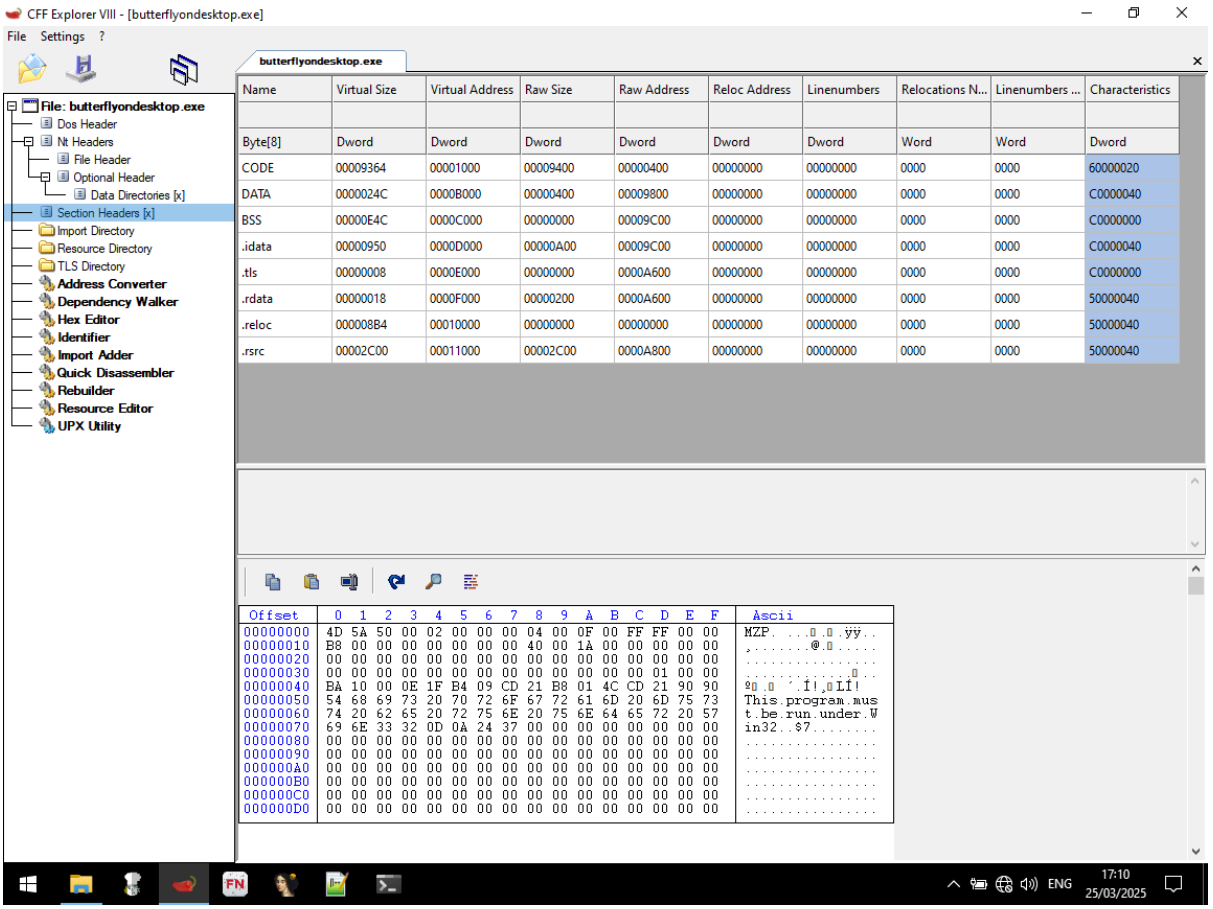

CFF Explorer VIII - [butterflyondesktop.exe]
File Settings ?
butterflyondesktop.exe
File: butterflyondesktop.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Property Value
File Name C:\Users\FlareVM\Desktop\Malware\Spyware\butterflyondesktop.exe
File Type Portable Executable 32
File Info Borland Delphi 4.0
File Size 2.85 MB (2986944 bytes)
PE Size 53.00 KB (54272 bytes)
Created Tuesday 25 March 2025, 14.44.26
Modified Tuesday 25 March 2025, 14.44.26
Accessed Tuesday 25 March 2025, 15.12.52
MD5 1535AA21451192109B86BE9BCC7C4345
SHA-1 1AF211C686C4D4BF0239ED6620358A19691CF88C
Property Value
Comments This installation was built with Inno Setup.
CompanyName Drive Software Company
FileDescription Butterfly on Desktop Setup
FileVersion
LegalCopyright
ProductName Butterfly on Desktop
ENG
15:13
25/03/2025


CFF Explorer VIII - [butterflyondesktop.exe]
File Settings ?
butterflyondesktop.exe
File: butterflyondesktop.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Name Virtual Size Virtual Address Raw Size Raw Address Reloc Address Linenumbers Relocations N... Linenumbers ... Characteristics
Byte[8] Dword Dword Dword Dword Dword Dword Word Word Dword
CODE 00009364 00001000 00009400 00000400 00000000 00000000 0000 0000 60000020
DATA 0000024C 0000B000 00000400 00009800 00000000 00000000 0000 0000 C0000040
BSS 00000E4C 0000C000 00000000 00009C00 00000000 00000000 0000 0000 C0000000
.idata 00000950 0000D000 00000A00 00009C00 00000000 00000000 0000 0000 C0000040
.tls 00000008 0000E000 00000000 0000A600 00000000 00000000 0000 0000 C0000000
.rdata 00000018 0000F000 00000200 0000A600 00000000 00000000 0000 0000 50000040
.reloc 000008B4 00010000 00000000 00000000 00000000 00000000 0000 0000 50000040
.rsrc 00002C00 00011000 00002C00 0000A800 00000000 00000000 0000 0000 50000040
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
00000000 4D 5A 50 00 02 00 00 00 04 00 0F 00 FF FF 00 00 MZP. ...▯.▯.ÿÿ..
00000010 B8 00 00 00 00 00 00 00 40 00 1A 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 01 00 00 00 ....▯...
00000040 BA 10 00 0E 1F B4 09 CD 21 B8 01 4C CD 21 90 90 º▯.▯.´.Í!¸▯LÍ!..
00000050 54 68 69 73 20 70 72 6F 67 72 61 6D 20 6D 75 73 This program mus
00000060 74 20 62 65 20 72 75 6E 20 75 6E 64 65 72 20 57 t be run under W
00000070 69 6E 33 32 0D 0A 24 37 00 00 00 00 00 00 00 00 in32..$7........
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
ENG
17:10
25/03/2025

Non sono riuscito a fare l’analisi dinaminca