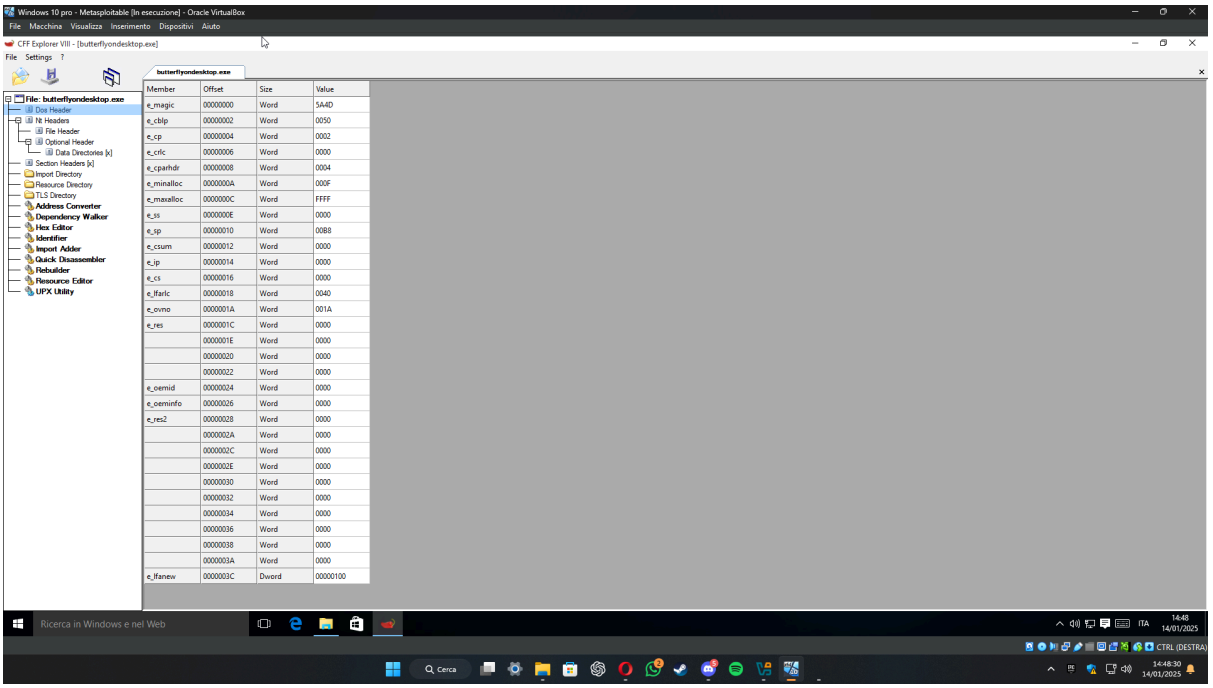
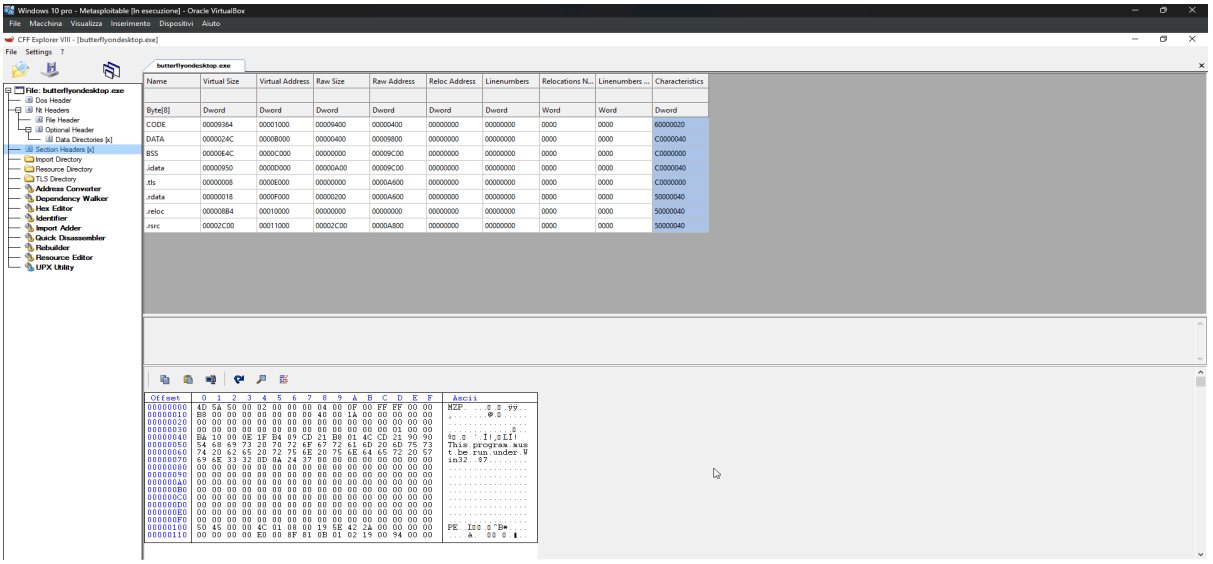
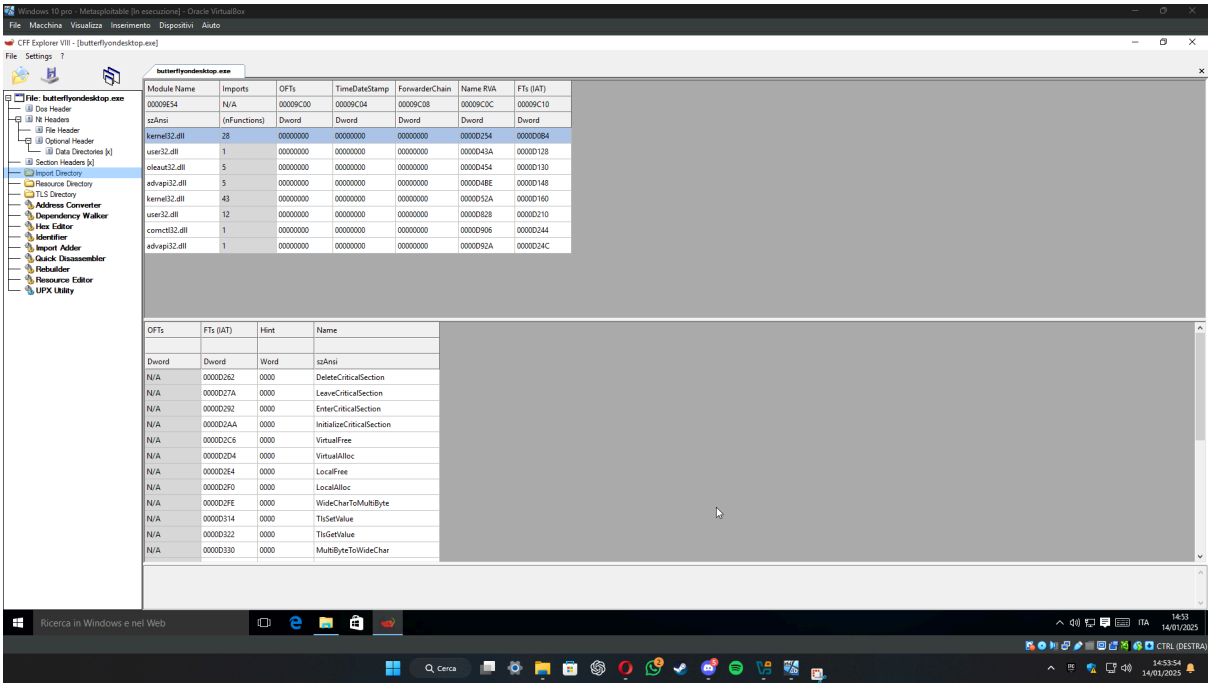
Attività di Analisi del Malware

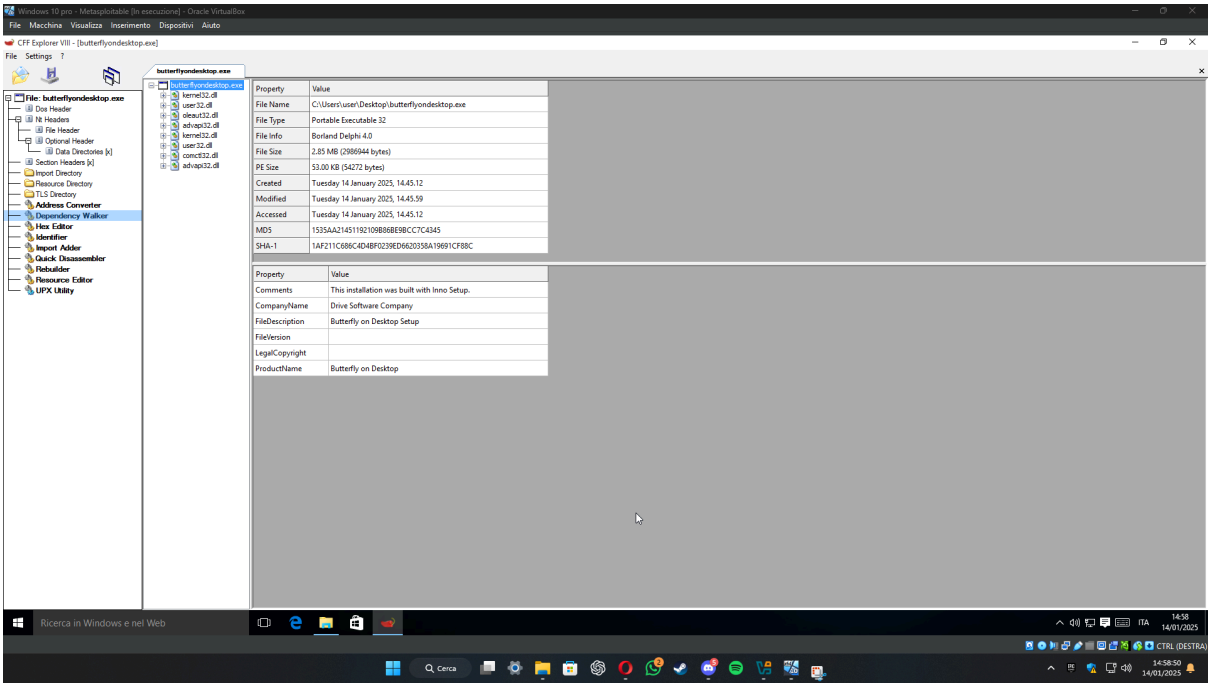
Analisi Statica:

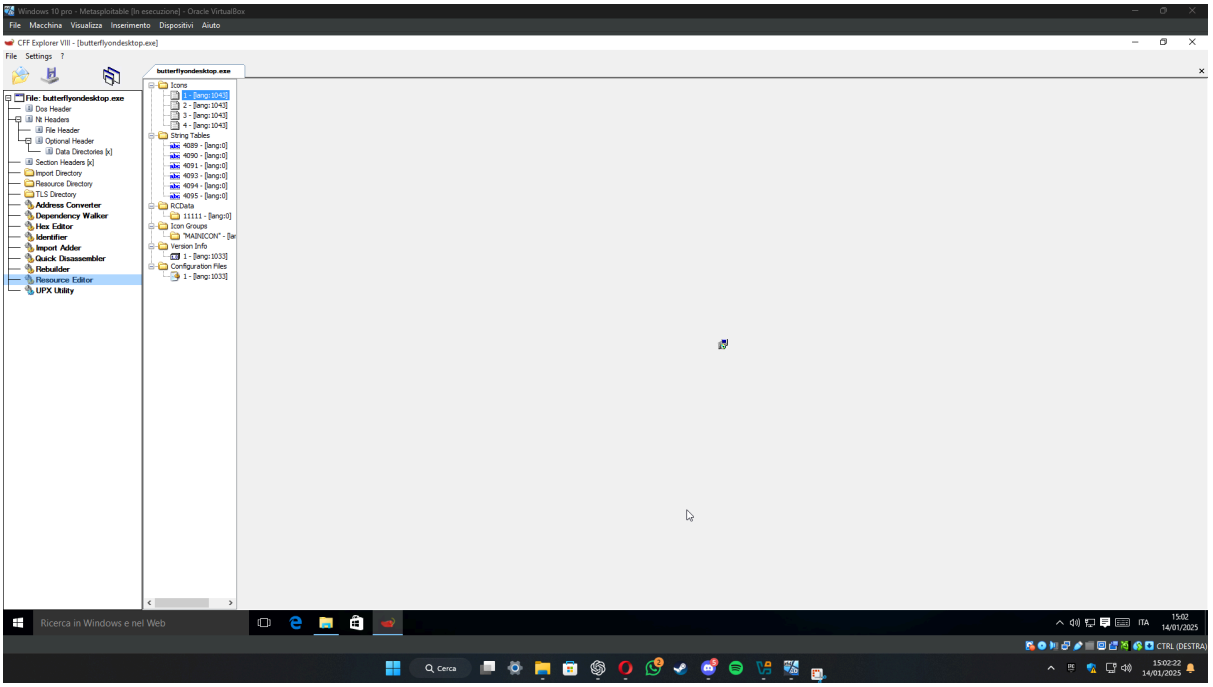




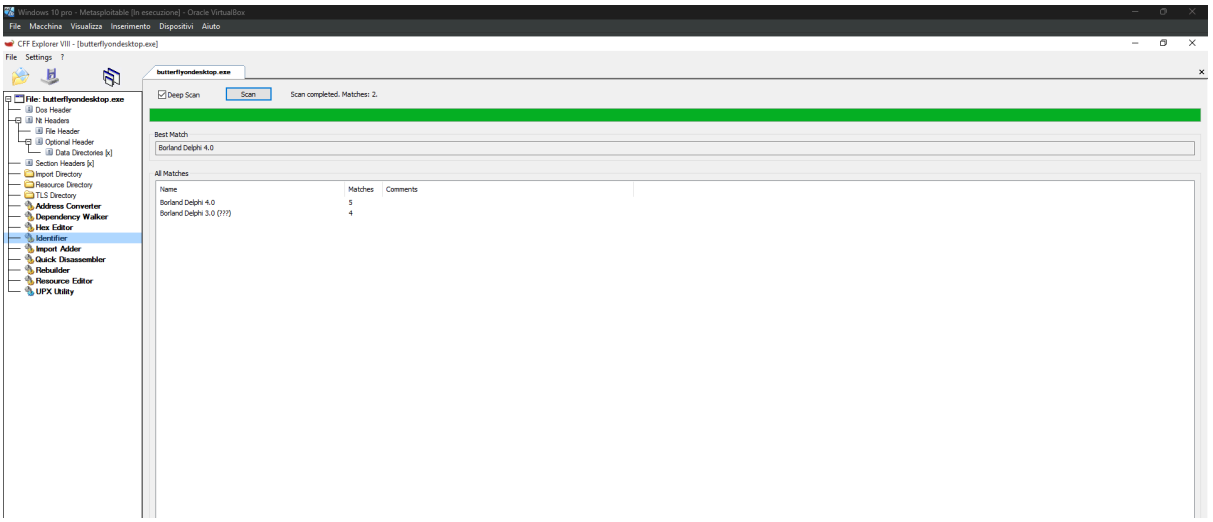
Da queste prime due foto possiamo trovare sia il codice 5A4D nella prima foto mentre nella seconda foto possiamo trovare le iniziali MZ nel linguaggio ASCII che sta ad indicare che è un file eseguibile


Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
00009E54 | N/A | 00009C00 | 00009C04 | 00009C08 | 00009C0C | 00009C10
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword
kernel32.dll | 28 | 00000000 | 00000000 | 00000000 | 0000D254 | 0000D0B4
user32.dll | 1 | 00000000 | 00000000 | 00000000 | 0000D43A | 0000D128
oleaut32.dll | 5 | 00000000 | 00000000 | 00000000 | 0000D454 | 0000D130
advapi32.dll | 5 | 00000000 | 00000000 | 00000000 | 0000D4BE | 0000D148
kernel32.dll | 43 | 00000000 | 00000000 | 00000000 | 0000D52A | 0000D160
user32.dll | 12 | 00000000 | 00000000 | 00000000 | 0000D828 | 0000D210
comctl32.dll | 1 | 00000000 | 00000000 | 00000000 | 0000D906 | 0000D244
advapi32.dll | 1 | 00000000 | 00000000 | 00000000 | 0000D92A | 0000D24C
OFTs | FTs (IAT) | Hint | Name
Dword | Dword | Word | szAnsi
N/A | 0000D262 | 0000 | DeleteCriticalSection
N/A | 0000D27A | 0000 | LeaveCriticalSection
N/A | 0000D292 | 0000 | EnterCriticalSection
N/A | 0000D2AA | 0000 | InitializeCriticalSection
N/A | 0000D2C6 | 0000 | VirtualFree
N/A | 0000D2D4 | 0000 | VirtualAlloc
N/A | 0000D2E4 | 0000 | LocalFree
N/A | 0000D2F0 | 0000 | LocalAlloc
N/A | 0000D2FE | 0000 | WideCharToMultiByte
N/A | 0000D314 | 0000 | TlsSetValue
N/A | 0000D322 | 0000 | TlsGetValue
N/A | 0000D330 | 0000 | MultiByteToWideChar
Ricerca in Windows e nel Web
ITA
14:53
14/01/2025
CTRL (DESTRA)
Cerca
14:53:54
14/01/2025


Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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
butterflyondesktop.exe
kernel32.dll
user32.dll
oleaut32.dll
advapi32.dll
kernel32.dll
user32.dll
comctl32.dll
advapi32.dll
Property | Value
File Name | C:\Users\user\Desktop\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 14 January 2025, 14.45.12
Modified | Tuesday 14 January 2025, 14.45.59
Accessed | Tuesday 14 January 2025, 14.45.12
MD5 | 1535AA21451192109BB6BE9BCC7C4345
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
Ricerca in Windows e nel Web
ITA
14:58
14/01/2025
CTRL (DESTRA)
Cerca
14:58:50
14/01/2025

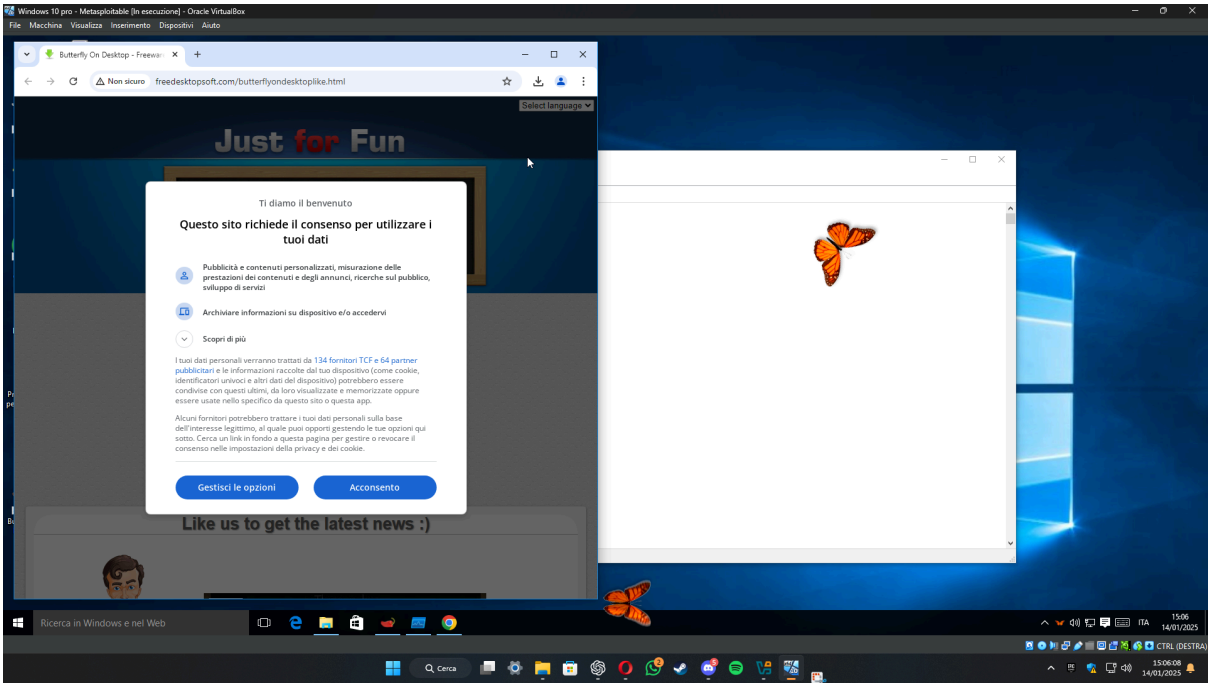


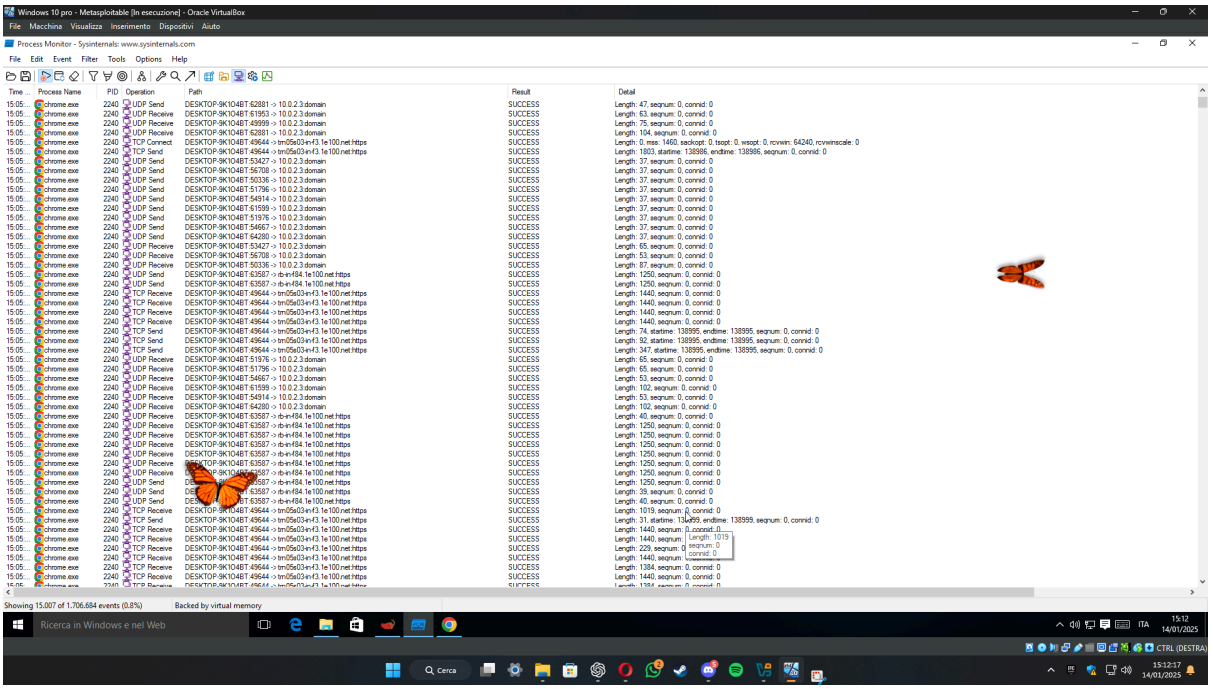
Da questa foto si può visualizzare invece la lingua delle icone in questo caso olandese (lang:1043) mentre per Version Info e Configuration File è scritto in inglese (lang: 1033)



Da quest'ultima invece ho avviato una scansione dandomi questi due file Borland Delphi V 4.0 e Borland Delphi V 3.0 e facendo una ricerca questi due file permettono di creare e compilare un codice malevolo, offuscare il codice e automatizzare azioni dannose.

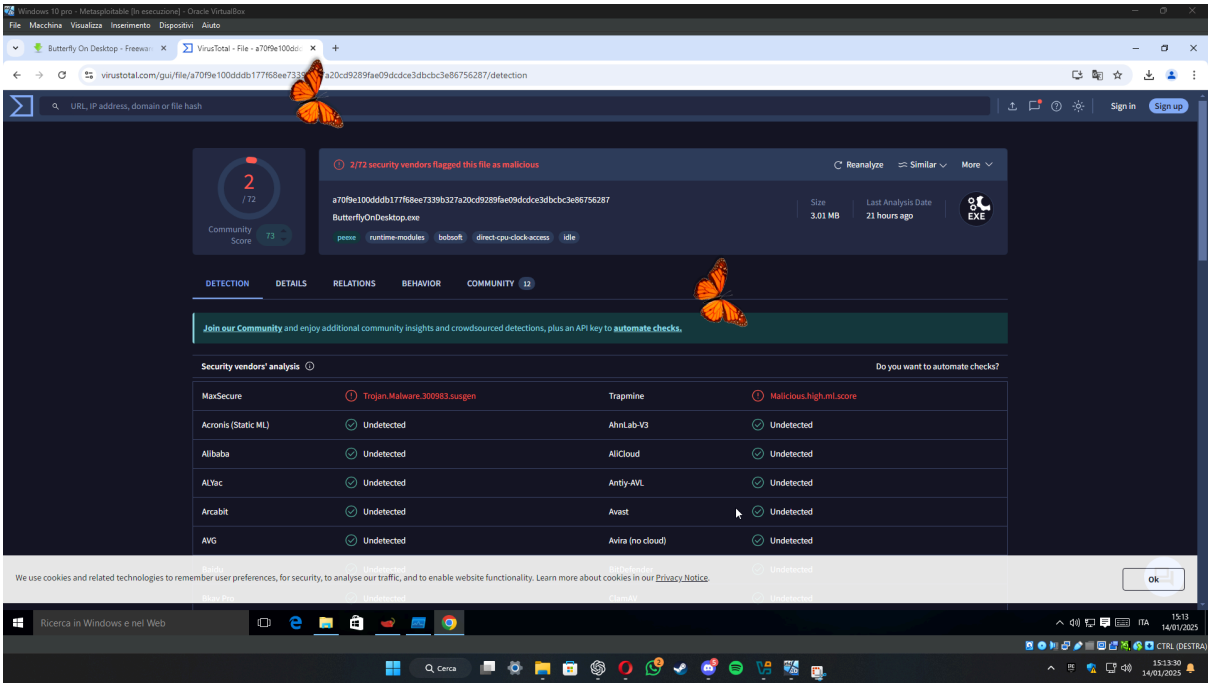
Analisi Dinamica:





Tramite l'utilizzo di Process Monitor ho analizzato le richieste una volta avviato il malware per prima cosa ho visto che mi riportava ad una pagina e ho analizzato anche le richieste di rete come si può vedere dalla seconda foto.

Analisi con viru total:



Facendo l'analisi nei file mi ha riscontrato un Trojan.