ANALISI STATICA

Per eseguire l'analisi statica del malware, utilizziamo CFF explorer, quindi, una volta scaricato il malware facciamo tasto destro e apriamo con il programma che ho menzionato:

Da qui abbiamo accesso ad alcune informazioni che ci permettono di analizzare il malware:

- File name
- File type
- File info
- PE size
- Created
- Modified
- Accessed
- MD5
- SHA-1

Property	Value
File Name	C:\Users\user\Downloads\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, 15.52.41
Modified	Tuesday 14 January 2025, 15.53.10
Accessed	Tuesday 14 January 2025, 15.52.41
MD5	1535AA21451192109B86BE9BCC7C4345
SHA-1	1AF211C686C4D4BF0239ED6620358A19691CF88C

Proseguiamo analizzando il Dos Header questo contiene la firma "MZ", che permette al sistema operativo di riconoscere il file come un eseguibile valido. Inoltre, contiene informazioni essenziali che vengono utilizzate quando il file viene caricato in memoria. In un'analisi di malware, verificare il DOS Header può aiutare a confermare l'integrità del file e a identificare eventuali manipolazioni. Passiamo alle sezioni principali del file:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
CODE	00009364	00001000	00009400	00000400	00000000	00000000	0000	0000
DATA	0000024C	0000B000	00000400	00009800	00000000	00000000	0000	0000
BSS	00000E4C	0000C000	00000000	00009C00	00000000	00000000	0000	0000
.idata	00000950	0000D000	00000A00	00009C00	00000000	00000000	0000	0000
.tls	00000008	0000E000	00000000	0000A600	00000000	00000000	0000	0000
.rdata	00000018	0000F000	00000200	0000A600	00000000	00000000	0000	0000
.reloc	000008B4	00010000	00000000	00000000	00000000	00000000	0000	0000
.rsrc	00002C00	00011000	00002C00	0000A800	00000000	00000000	0000	0000

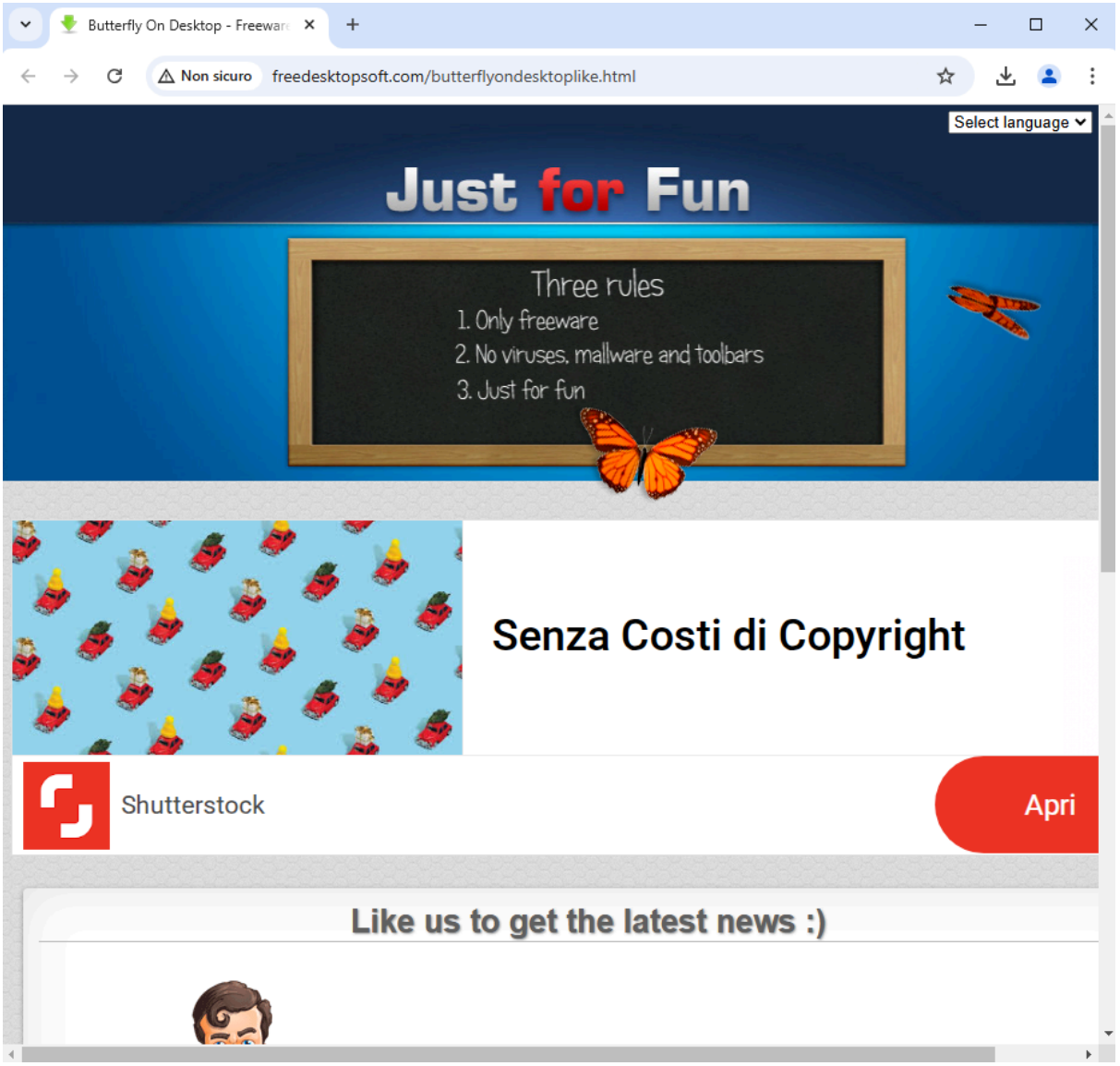
Poi analizziamo le import Directory:

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
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

KERNEL32.dll e USER32.dll sono critiche per il funzionamento del malware poiché forniscono accesso a funzioni di sistema fondamentali. ADVAPI32.dll indica che il malware potrebbe interagire con il registro di Windows, servizi di sistema e funzioni di sicurezza. SHELL32.dll e COMCTL32.dll suggeriscono che il malware potrebbe avere componenti di interfaccia utente o interagire con il filesystem di Windows.

ANALISI DINAMICA

Prima di tutto ci preoccupiamo di prepare un ambiente sicuro dove poter eseguire il malware senza paura di incorrere in conseguenze dannose dovute dall'esecuzione del malware. Quindi eseguiamo il malware e proviamo e tenere sotto controllo i processi con process monitor; una volta installato il malware appaiono delle farfalle sullo schermo ma soprattutto si apre una pagina html:



non sono riuscito ad analizzare bene i processi stavo diventando matto erano troppi 🙂