Esercizio.

Attività di Analisi del Malware

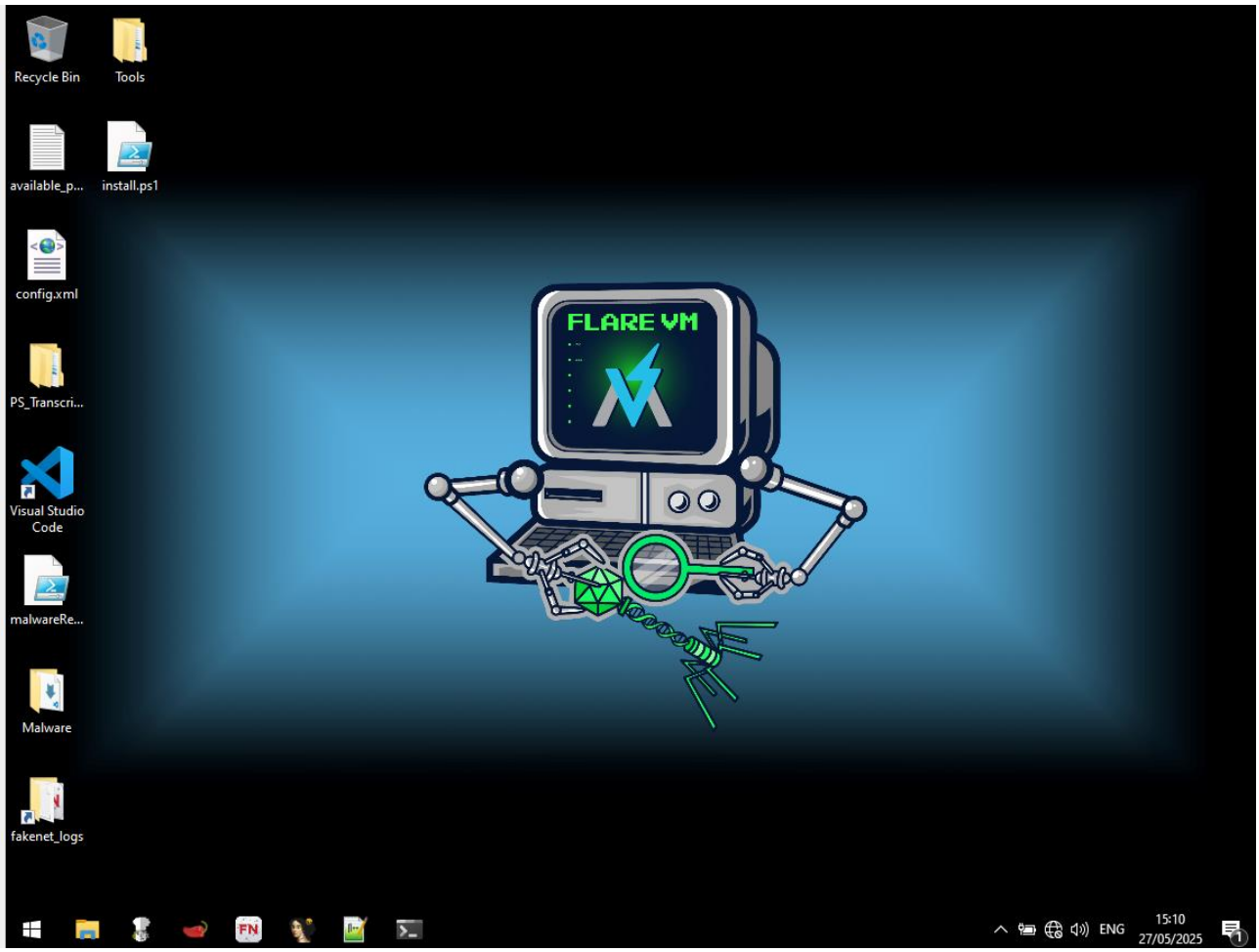
Oggetto: Sarà condiviso un malware relativamente innocuo.

Compiti:

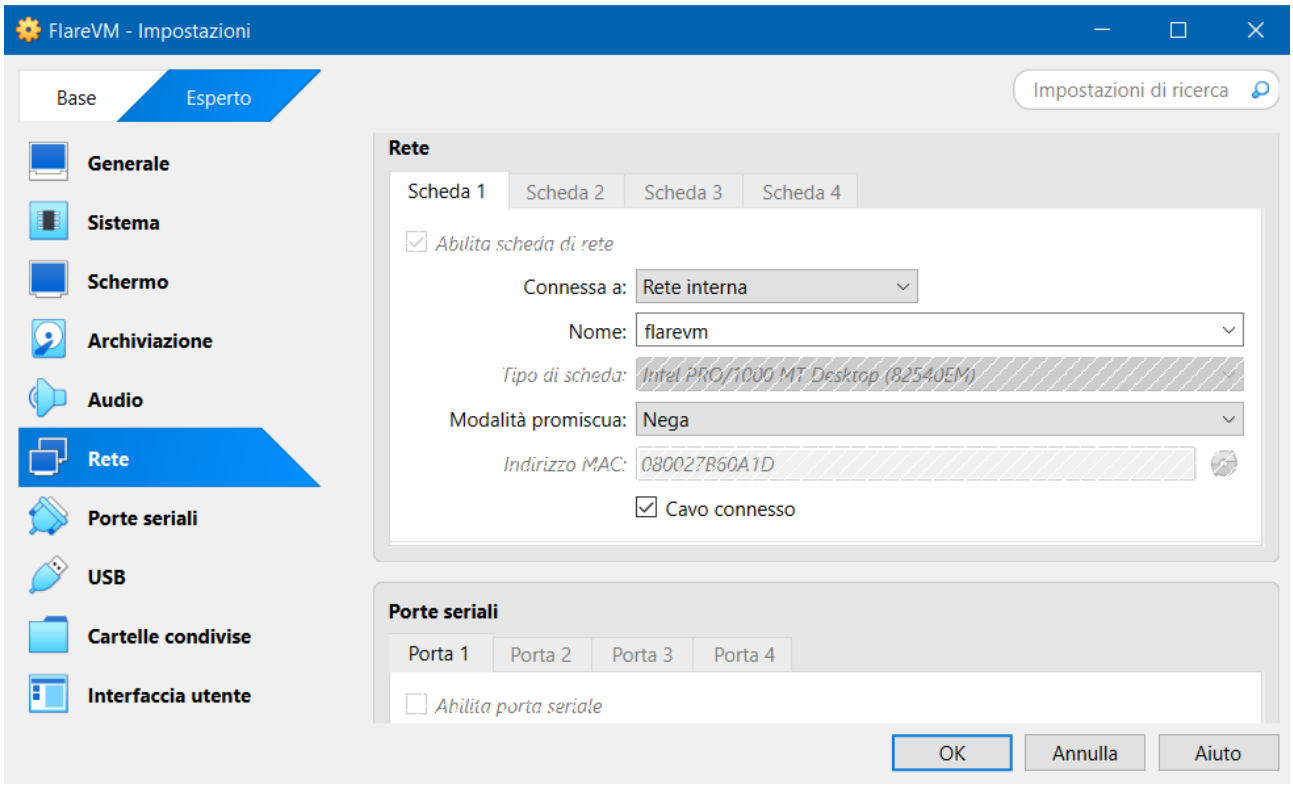
1. **Analisi Statica:** Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
2. **Analisi Dinamica:** Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Analisi statica con CFF Explorer.

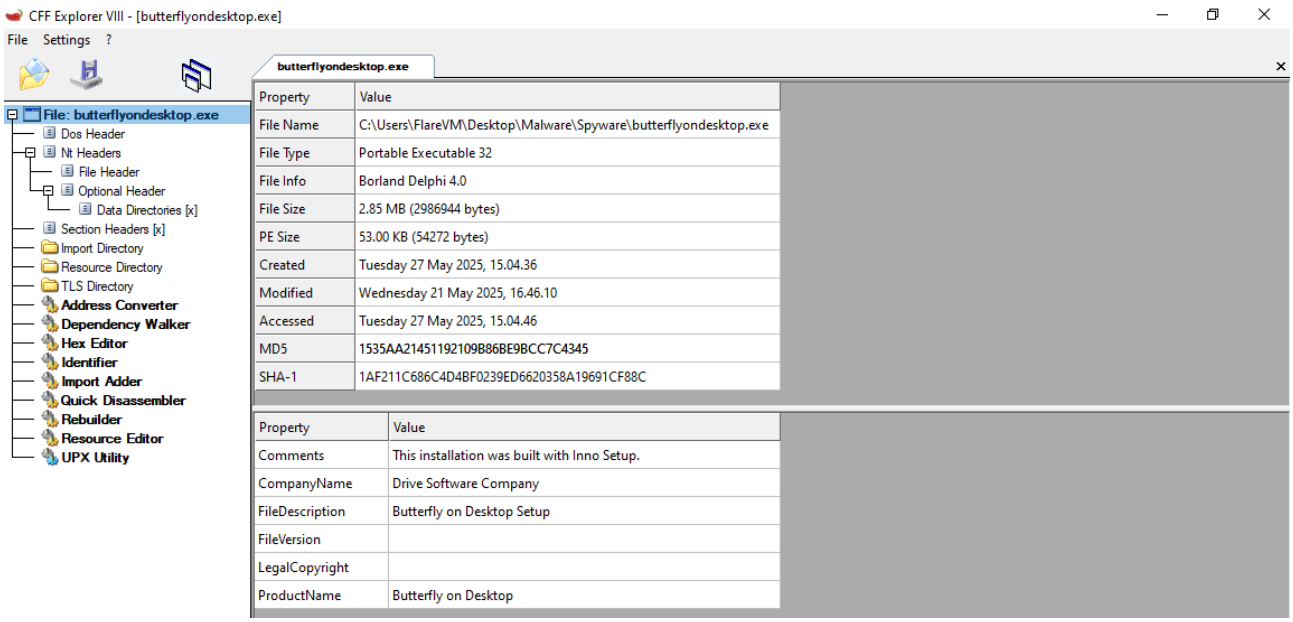
Ci assicuriamo che la macchina non sia connessa a internet



Scheda di rete:

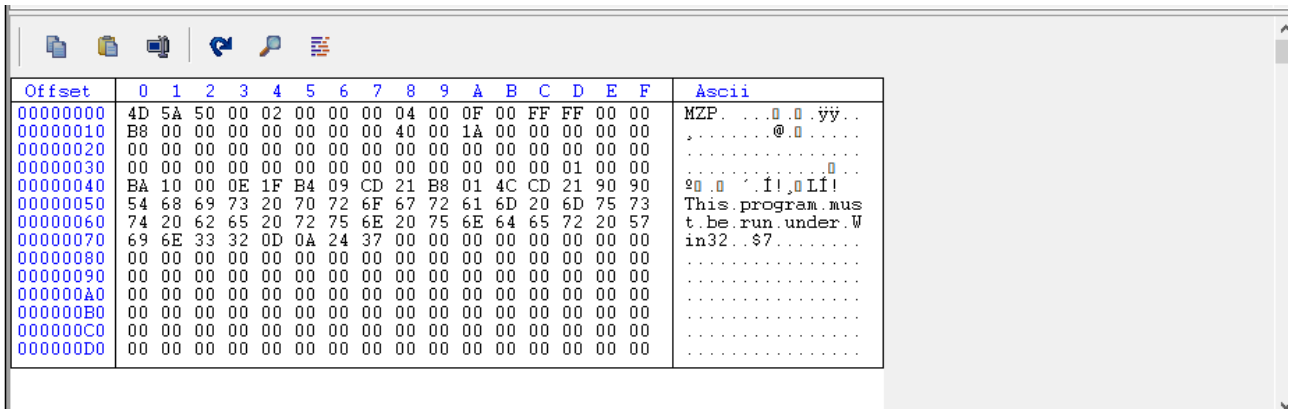


Una volta che ce ne siamo assicurati andremo ad analizzare lo spyware butterflyondesktop.exe

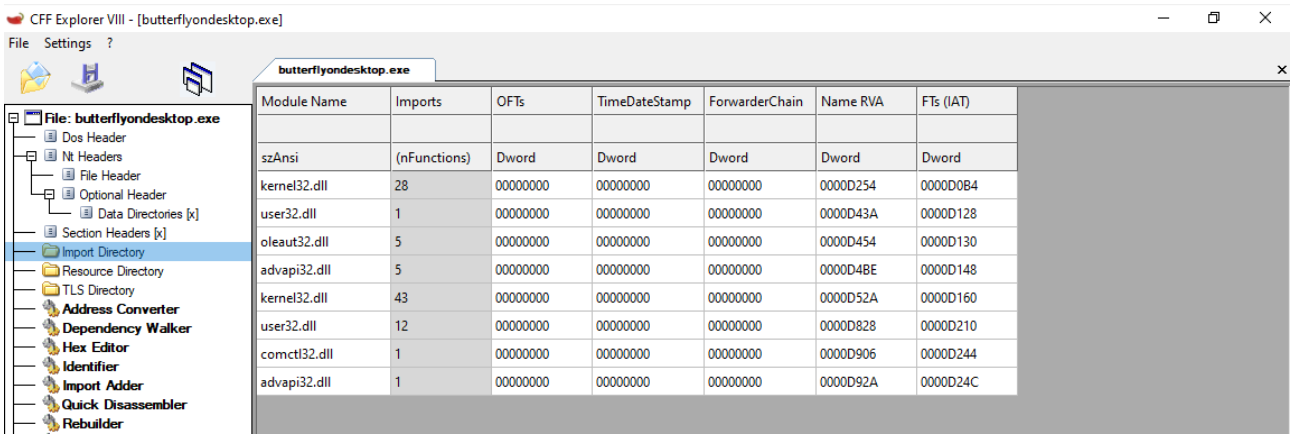


Ci sono molte informazioni interessanti quali: la dimensione del file, il tipo di file, la dimensione dell'header, l'hash MD5 del file e l'hash SHA-1.

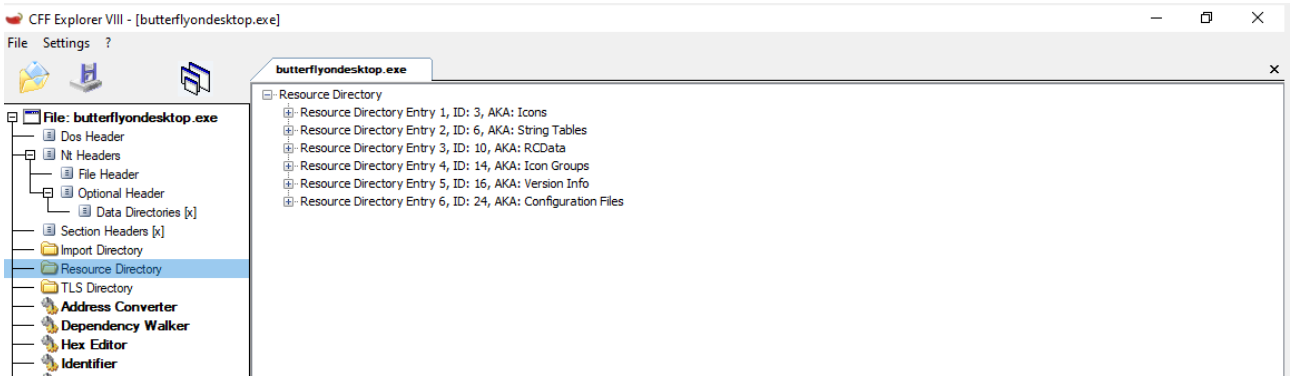
Nella sezione "Section Header" troviamo l'Ascii con firma MZ che permette al sistema operativo di riconoscere il file come eseguibile valido.



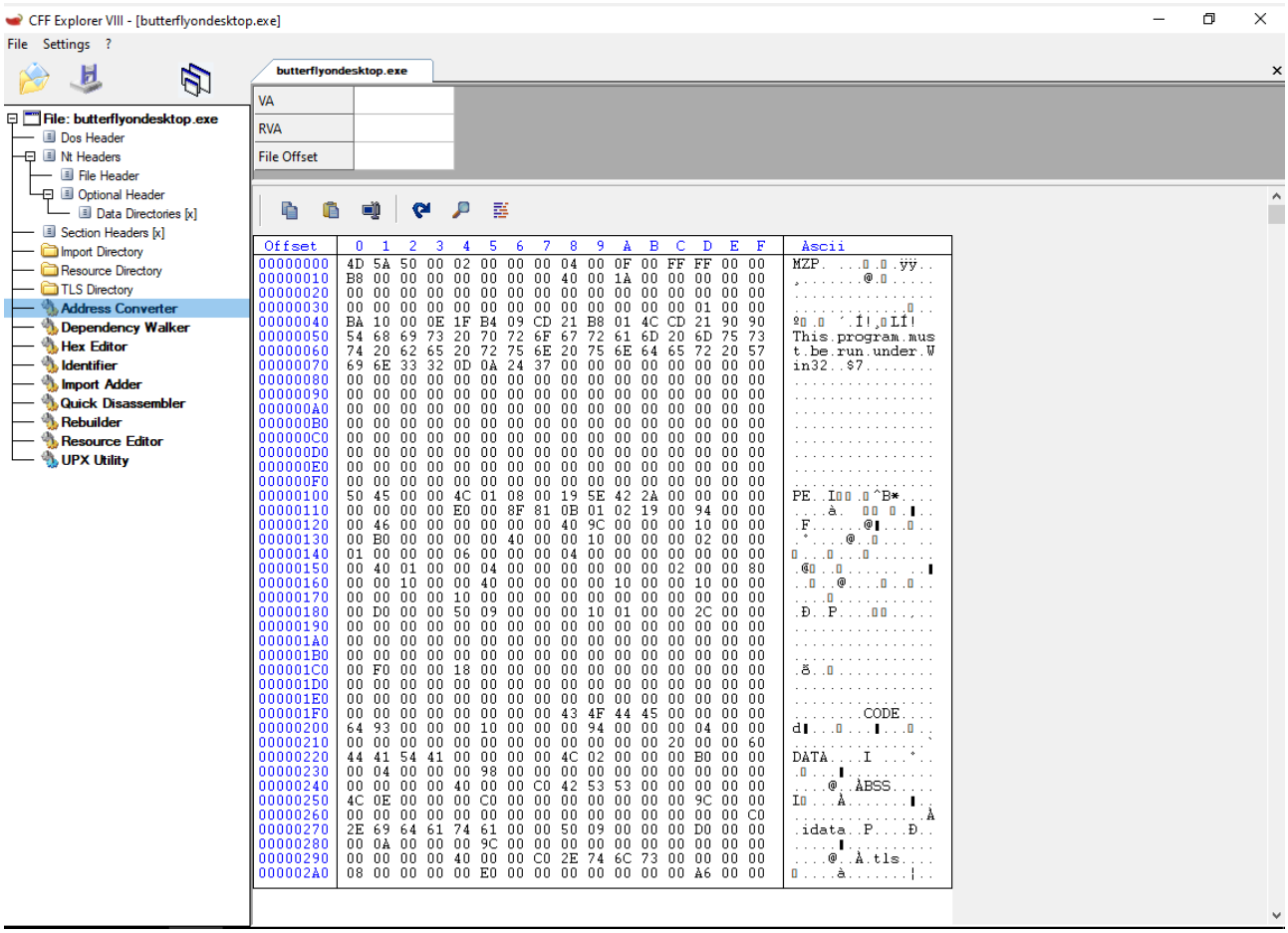
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	50	00	02	00	00	00	04	00	0F	00	FF	FF	00	00	MZP. ...□ .□ .ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	1A	00	00	00	00	00	¸.......@.□ .....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	01	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	....



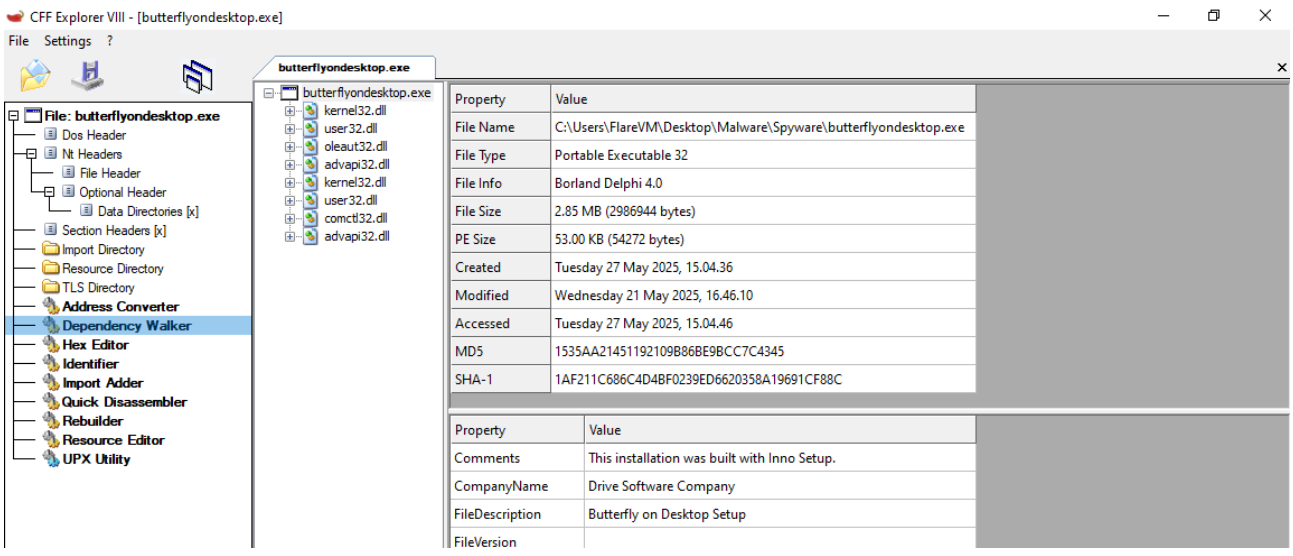
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
kernel32.dll	28	00000000	00000000	00000000	0000D254	0000D0B4
user32.dll	1	00000000	00000000	00000000	0000D43A	0000D128
oleaut32.dll	5	00000000	00000000	00000000	0000D454	0000D130
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



Codice eseguibile del malware.

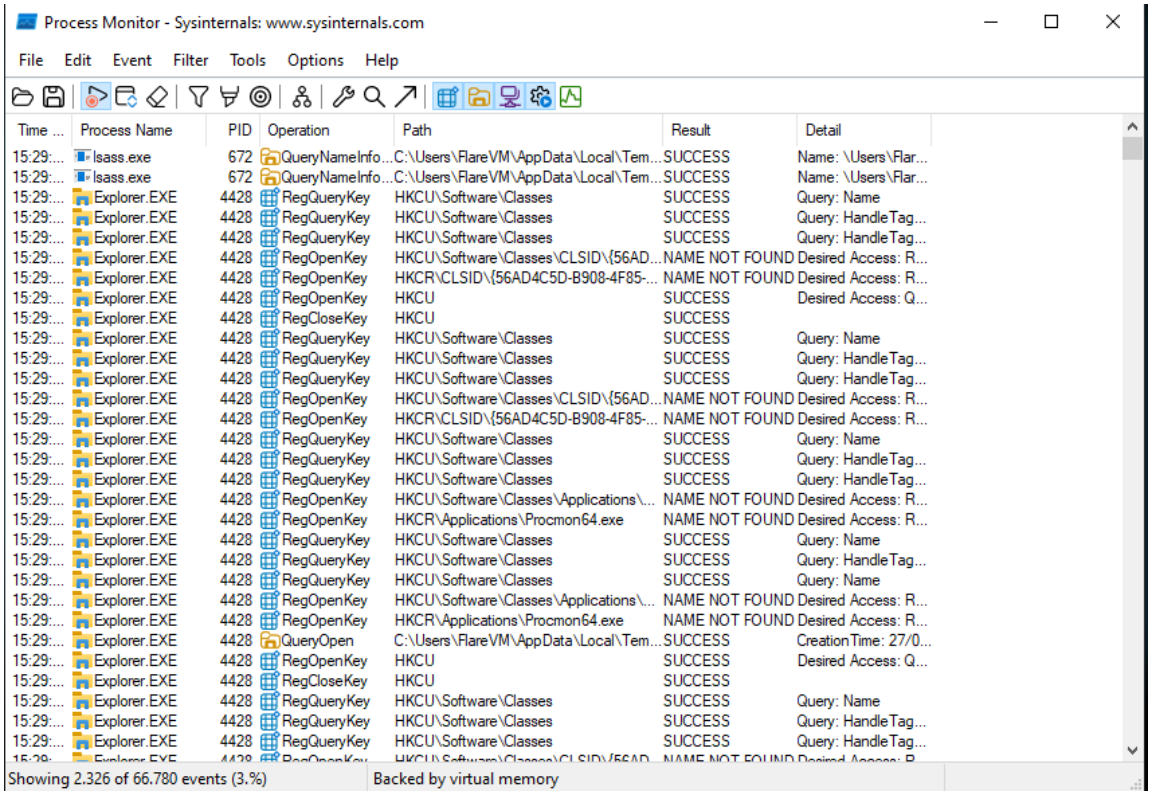


Librerie da cui dipende il codice

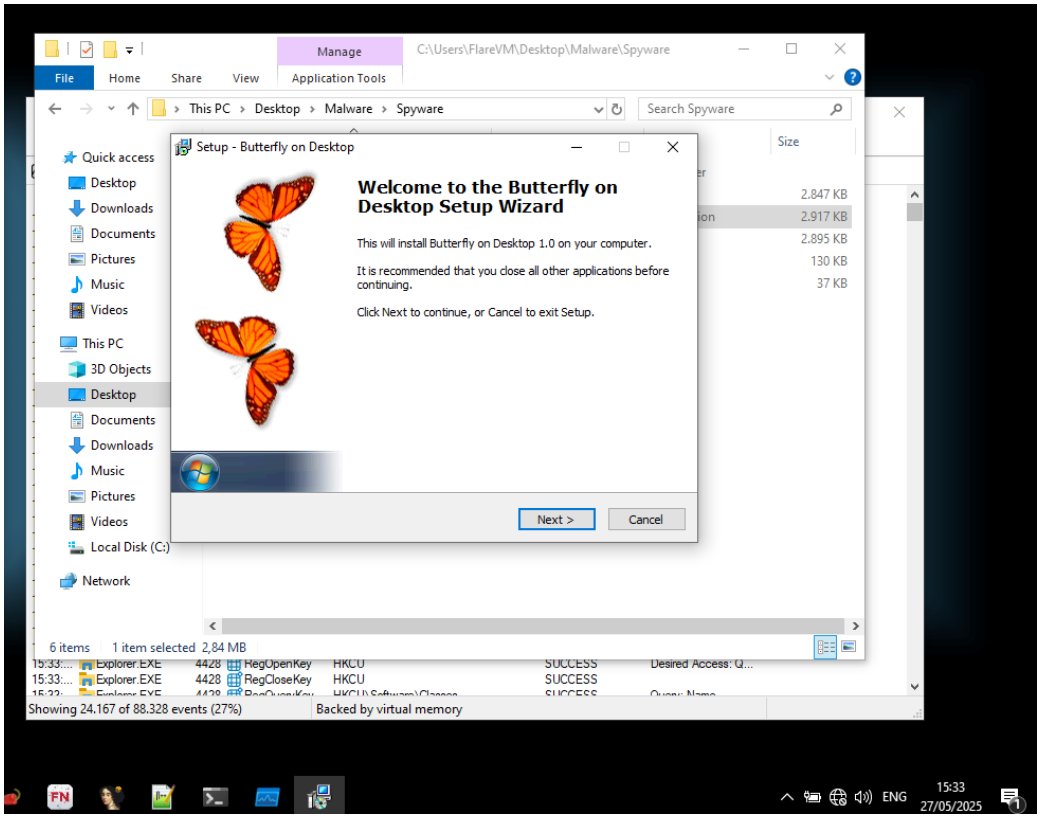


Analisi dinamica.

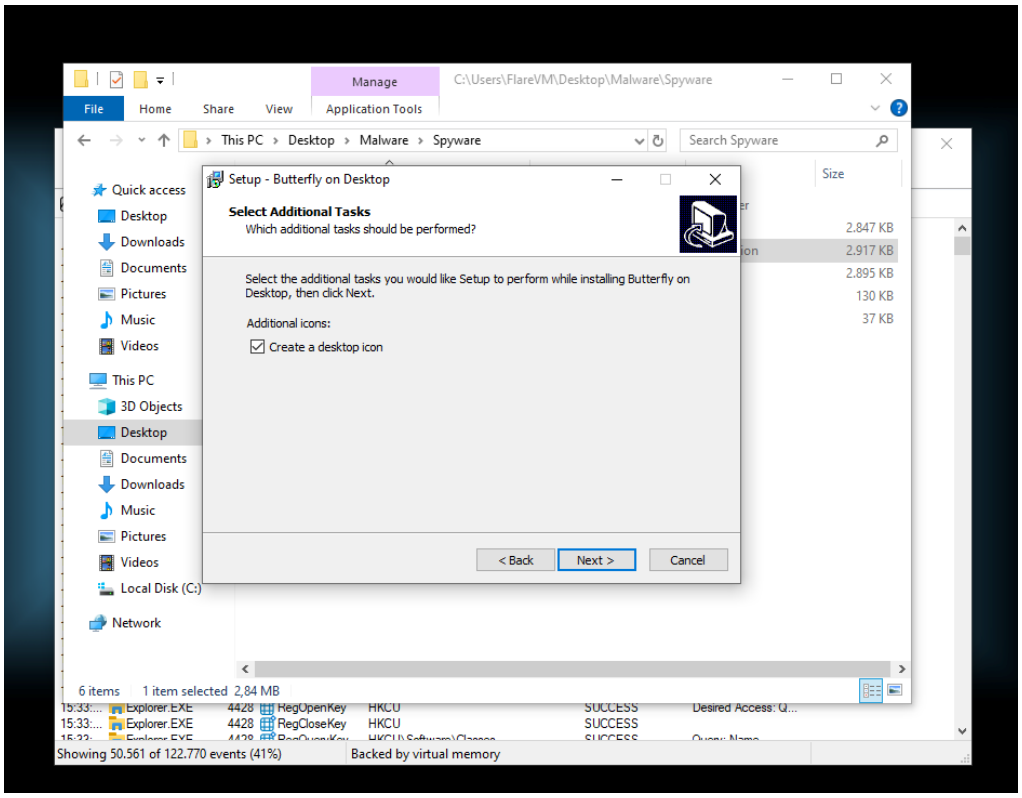
Apriamo Procrom64

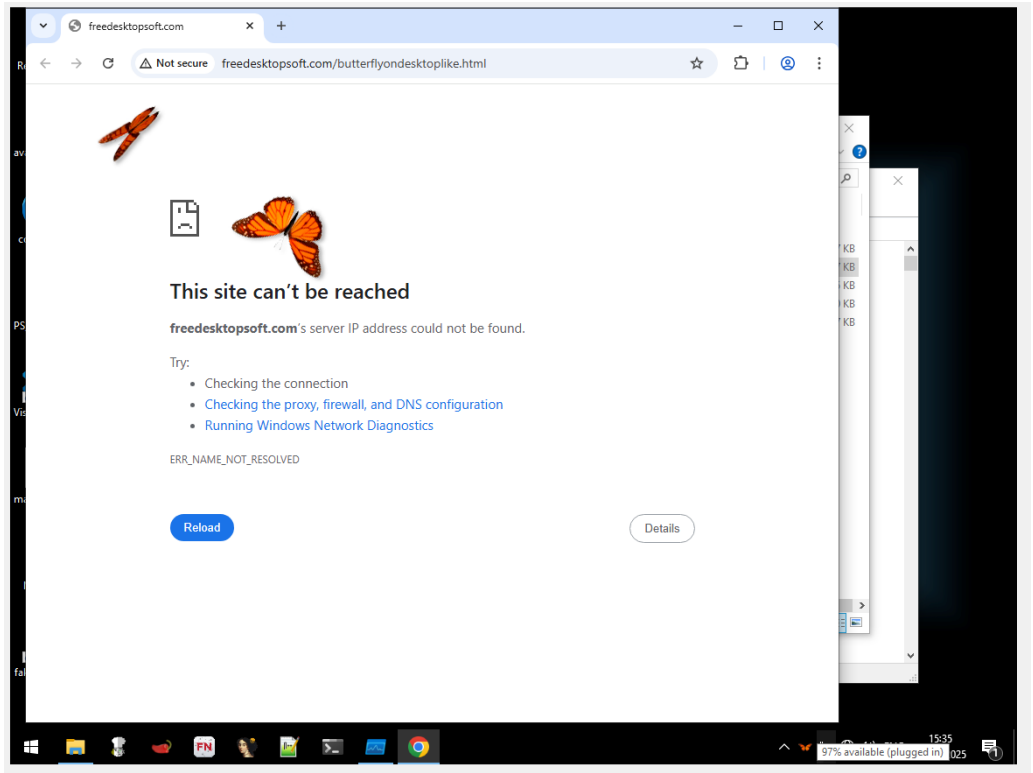


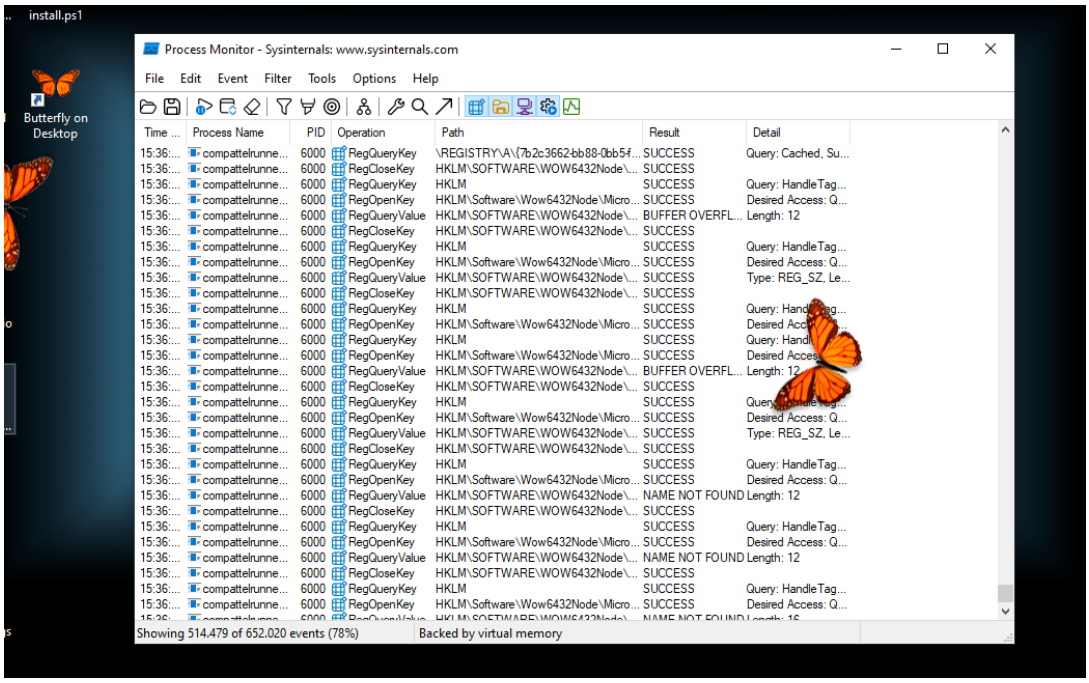
Avviamo lo spyware



Creiamo un’icona sul desktop

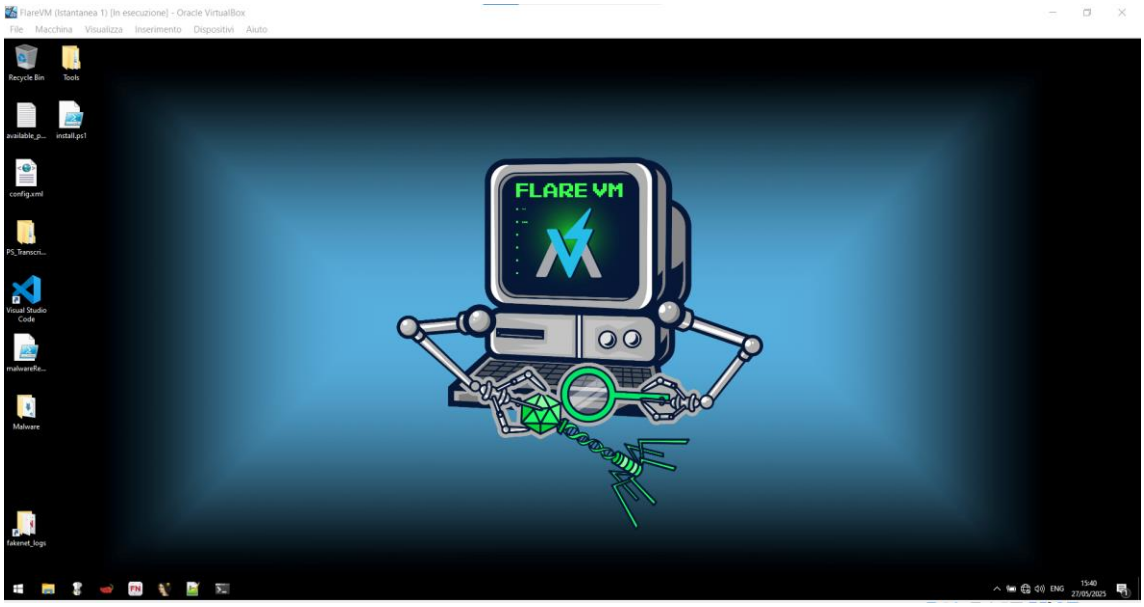






Noto che ci sono dei Buffer overflow

Finito l'esperimento ripristino tutto con l'istantanea creata prima di avviare lo spyware.



La macchina è stata ripristinata correttamente.