

Esercizio.

Attività di Analisi del Malware

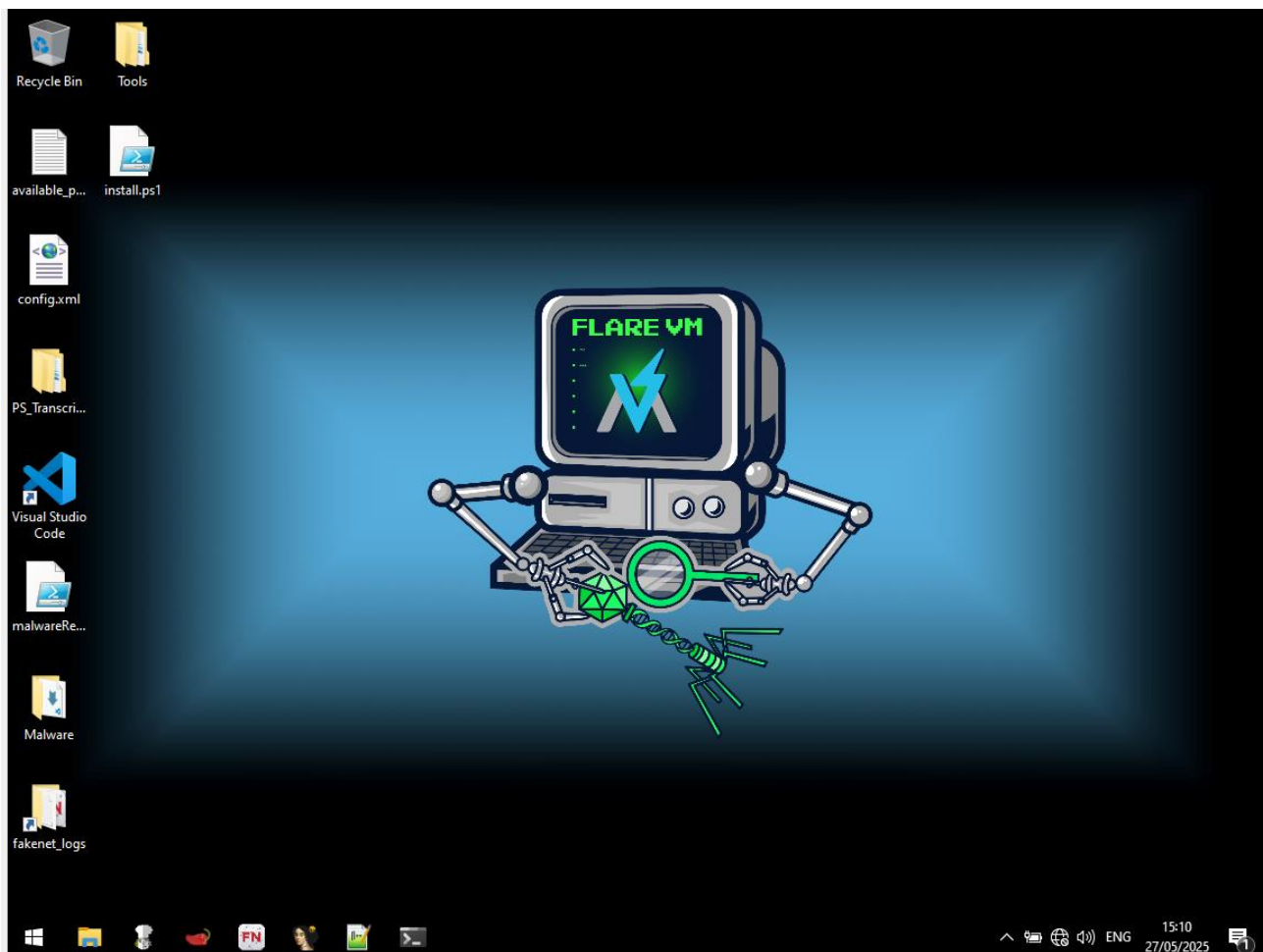
Oggetto: Sarà condiviso un malware relativamente innocuo.

Compiti:

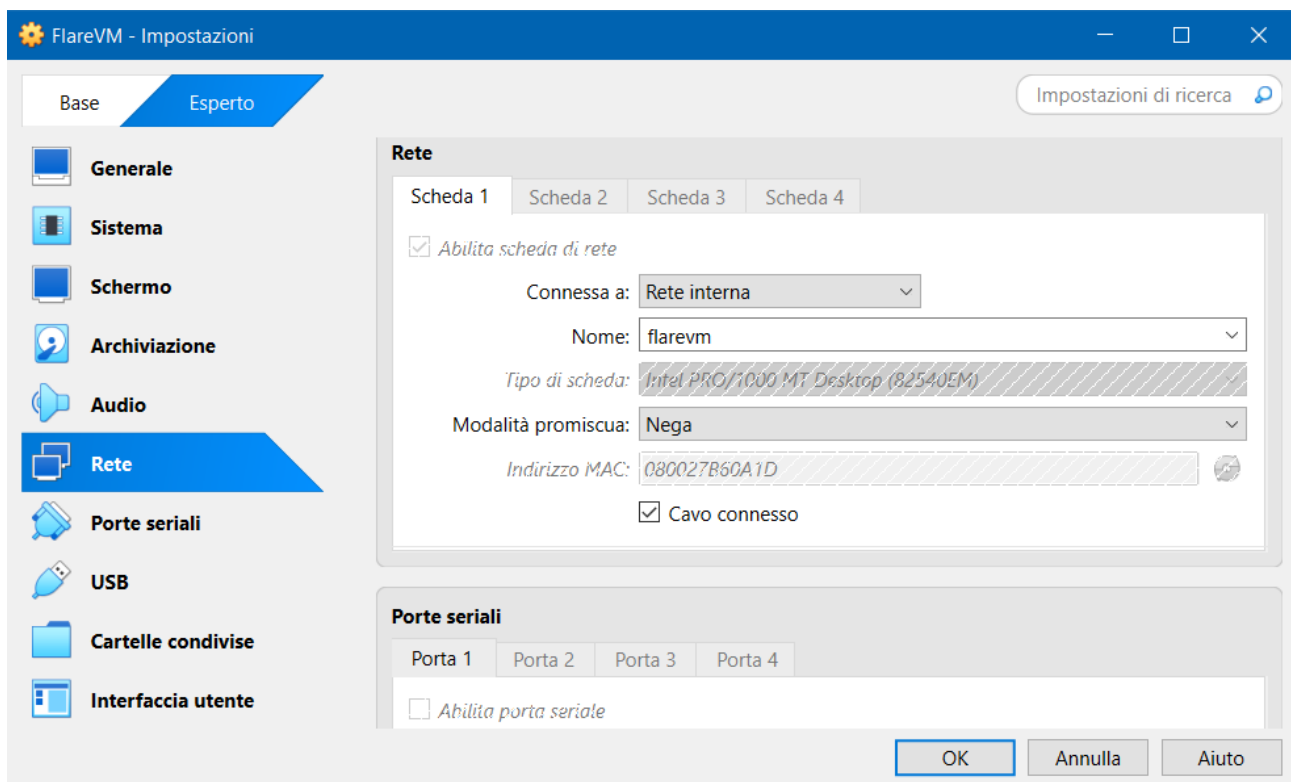
1. **Analisi Statica:** Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
2. **Analisi Dinamica:** Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Analisi statica con CFF Explorer.

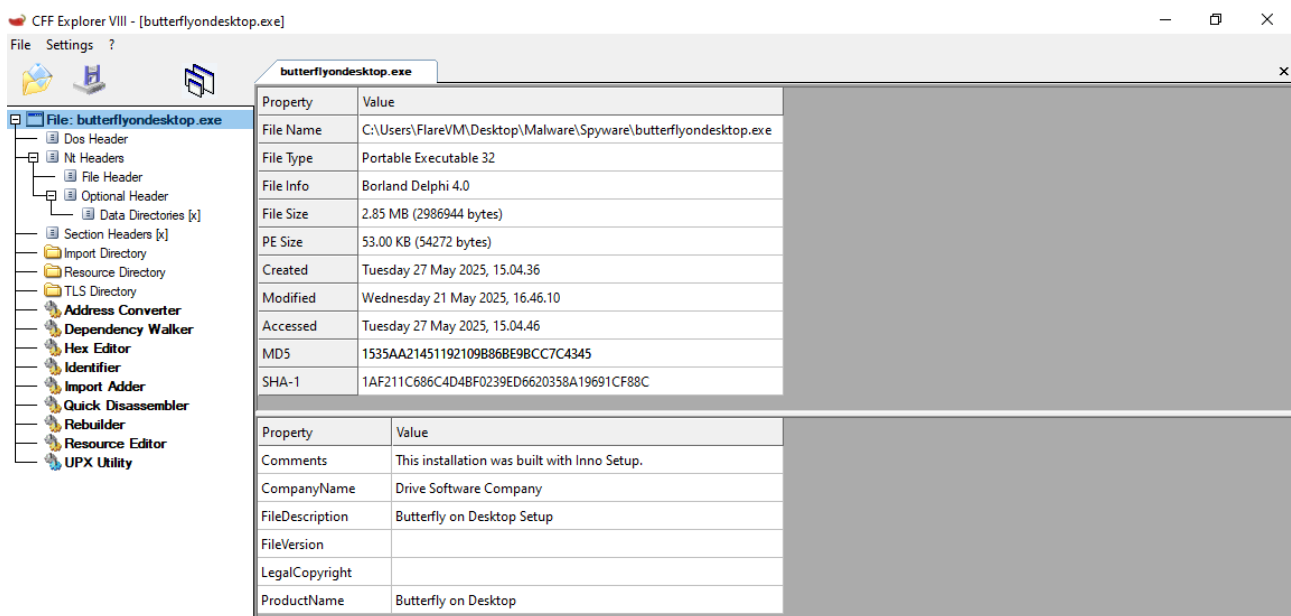
Ci assicuriamo che la macchina non sia connessa a internet



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...
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	%...!...!
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..\$?.....
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

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Module Name	Imports	OFs	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

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

Resource Directory

- Resource Directory Entry 1, ID: 3, AKA: Icons
- Resource Directory Entry 2, ID: 6, AKA: String Tables
- Resource Directory Entry 3, ID: 10, AKA: RCData
- Resource Directory Entry 4, ID: 14, AKA: Icon Groups
- Resource Directory Entry 5, ID: 16, AKA: Version Info
- Resource Directory Entry 6, ID: 24, AKA: Configuration Files

Codice eseguibile del malware.

CFF Explorer VIII - [butterflyondesktop.exe]

File Settings ?

butterflyondesktop.exe

VA
RVA
File Offset

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 Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

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	MZF.....yy..
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	q.....LI
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
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	50	45	00	00	4C	01	08	00	19	5E	42	2A	00	00	00	00	PE..I.....^B*
00000110	00	00	00	00	E0	00	8F	81	0B	01	02	19	00	94	00	00	..A.....
00000120	00	46	00	00	00	00	00	40	9C	00	00	00	10	00	00	00	.F.....@.....
00000130	00	B0	00	00	00	00	00	40	00	00	10	00	00	02	00	00@.....
00000140	01	00	00	00	06	00	00	04	00	00	00	00	00	00	00	00
00000150	00	40	01	00	00	04	00	00	00	00	00	02	00	00	80	00
00000160	00	00	10	00	00	40	00	00	00	10	00	00	10	00	00	00@.....
00000170	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000180	00	D0	00	00	50	09	00	00	10	01	00	00	2C	00	00	00	..P.....
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001C0	00	F0	00	00	18	00	00	00	00	00	00	00	00	00	00	00	..S.....
000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001F0	00	00	00	00	00	00	00	43	4F	44	45	00	00	00	00	00CODE.....
00000200	64	93	00	00	10	00	00	00	94	00	00	00	04	00	00	00	d.....I.....
00000210	00	00	00	00	00	00	00	00	00	00	20	00	00	60	00	00
00000220	44	41	54	41	00	00	00	4C	02	00	00	00	B0	00	00	00	DATA.....I.....
00000230	00	04	00	00	98	00	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	40	00	00	C0	42	53	53	00	00	00	00	00@..ABSS.....
00000250	4C	0E	00	00	00	C0	00	00	00	00	00	00	00	9C	00	00	I.....A.....
00000260	00	00	00	00	00	00	00	00	00	00	00	00	00	00	C0	00
00000270	2E	69	64	61	74	61	00	00	50	09	00	00	D0	00	00	00	..idata..P.....B.....
00000280	00	0A	00	00	9C	00	00	00	00	00	00	00	00	00	00	00@..A..tIs.....
00000290	00	00	00	00	40	00	00	C0	2E	74	6C	73	00	00	00	00@.....
000002A0	08	00	00	00	00	E0	00	00	00	00	00	00	A6	00	00	00@.....

Librerie da cui dipende il codice

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 Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

butterflyondesktop.exe

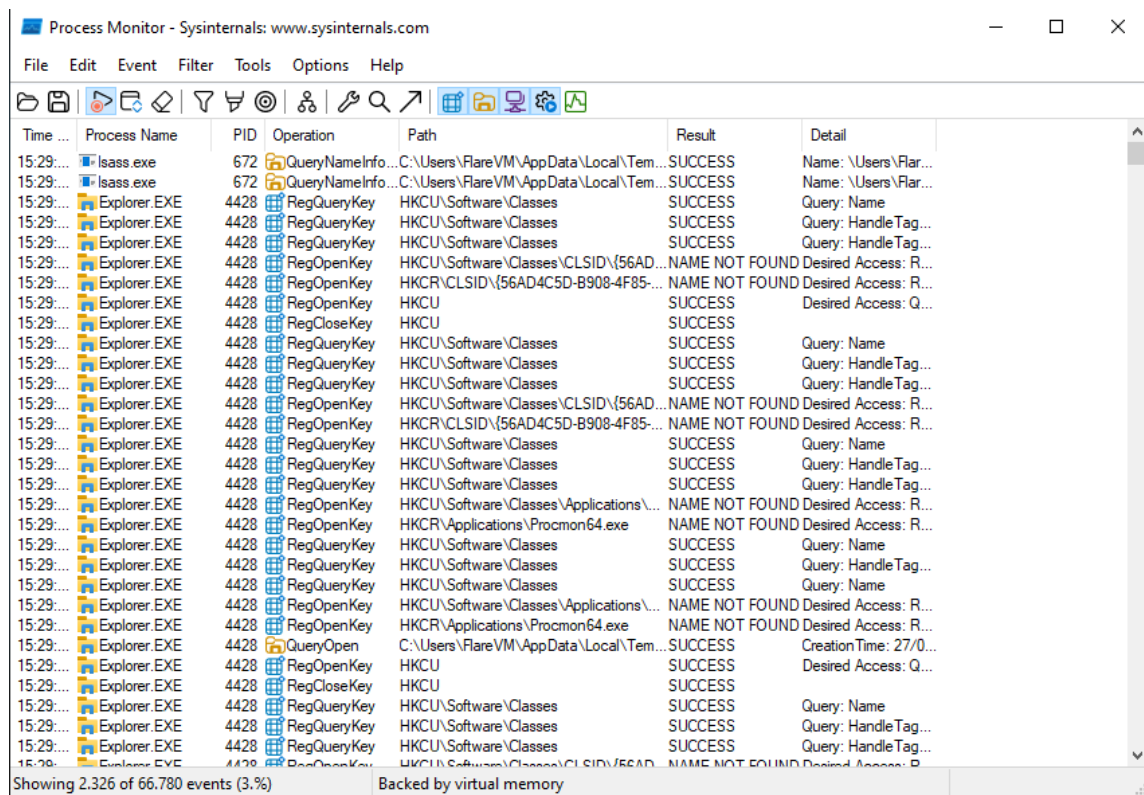
- kernel32.dll
- user32.dll
- oleaut32.dll
- advapi32.dll
- kernel32.dll
- user32.dll
- comctl32.dll
- advapi32.dll

Property	Value
File Name	C:\Users\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 27 May 2025, 15.04.36
Modified	Wednesday 21 May 2025, 16.46.10
Accessed	Tuesday 27 May 2025, 15.04.46
MD5	1535AA21451192109B86BE9BCC7C4345
SHA-1	1AF211C686C4D4BF0239ED6620358A19691CF88C

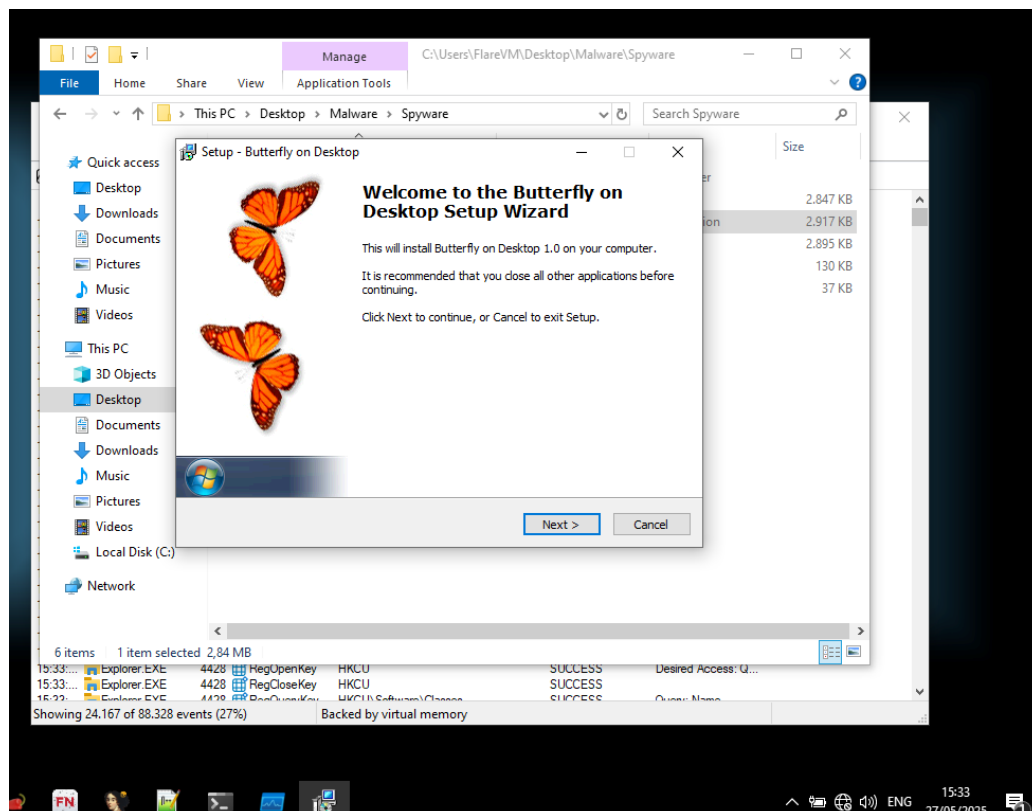
Property	Value
Comments	This installation was built with Inno Setup.
CompanyName	Drive Software Company
FileDescription	Butterfly on Desktop Setup
FileVersion	

Analisi dinamica.

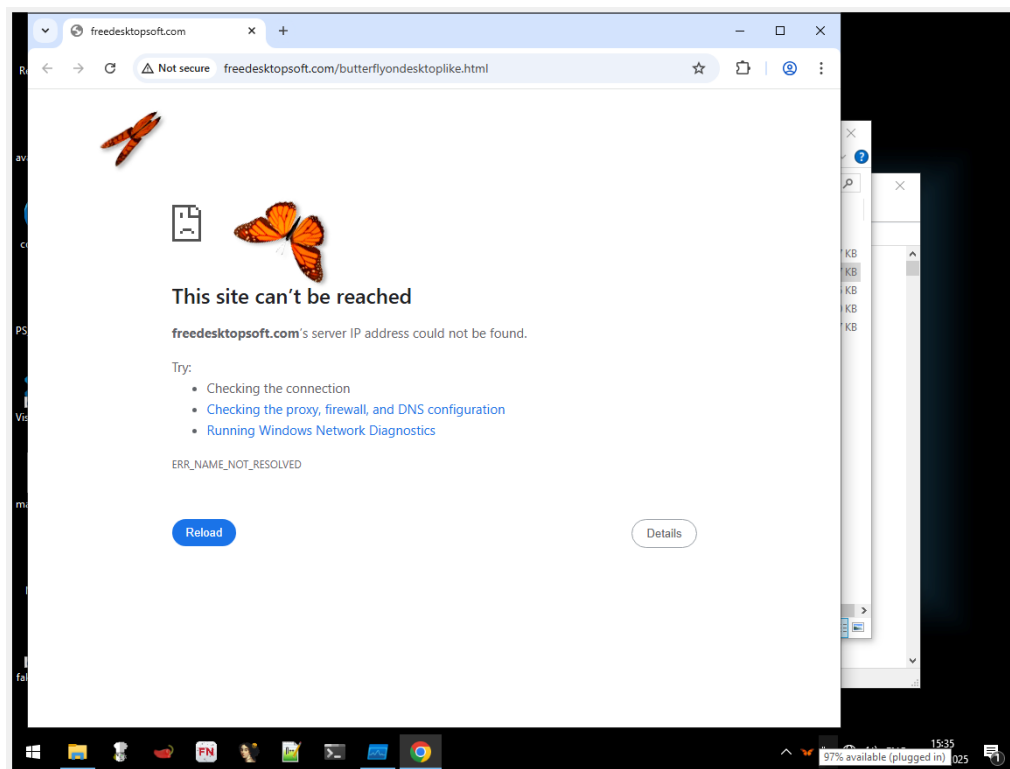
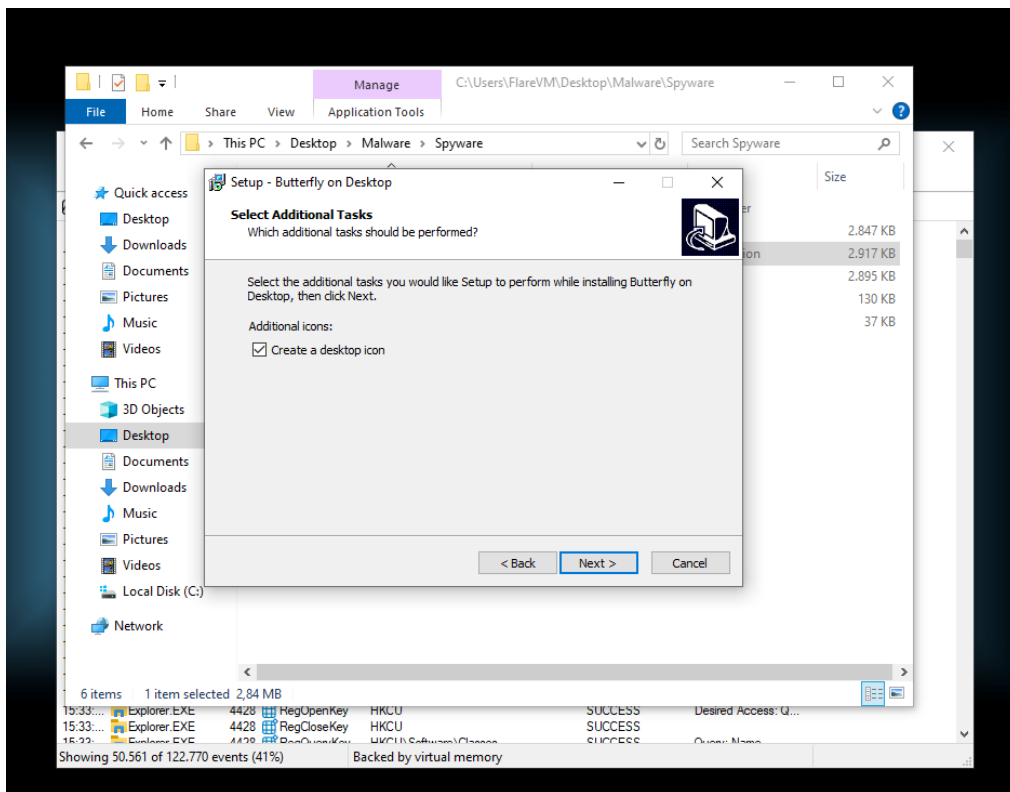
Apriamo Procrom64

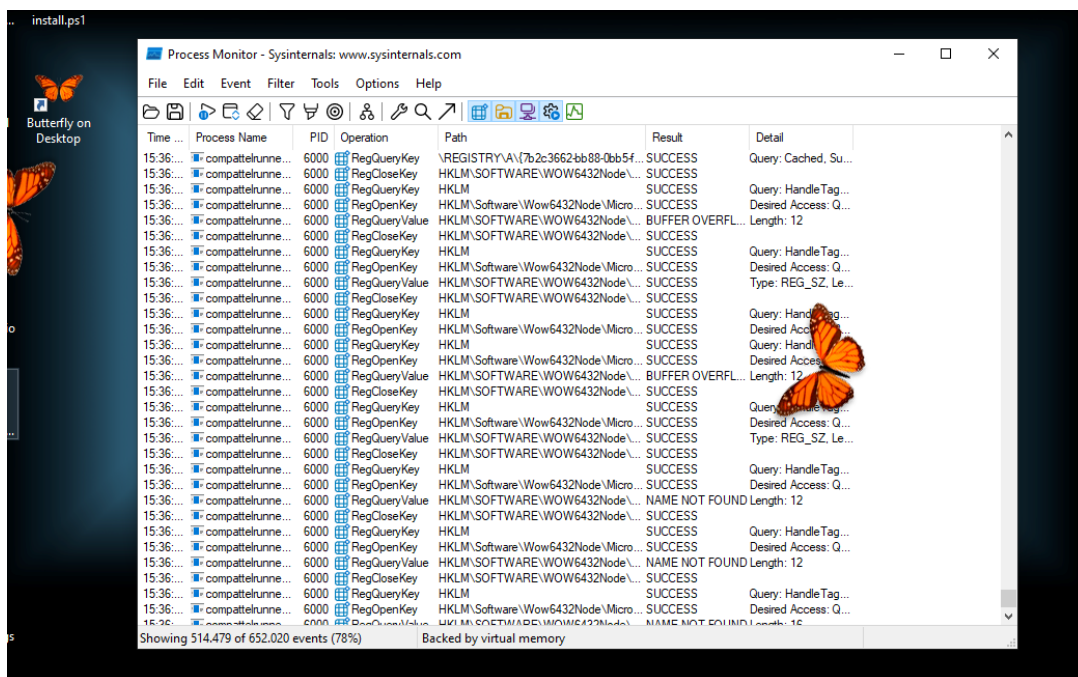


Avviamo lo spyware



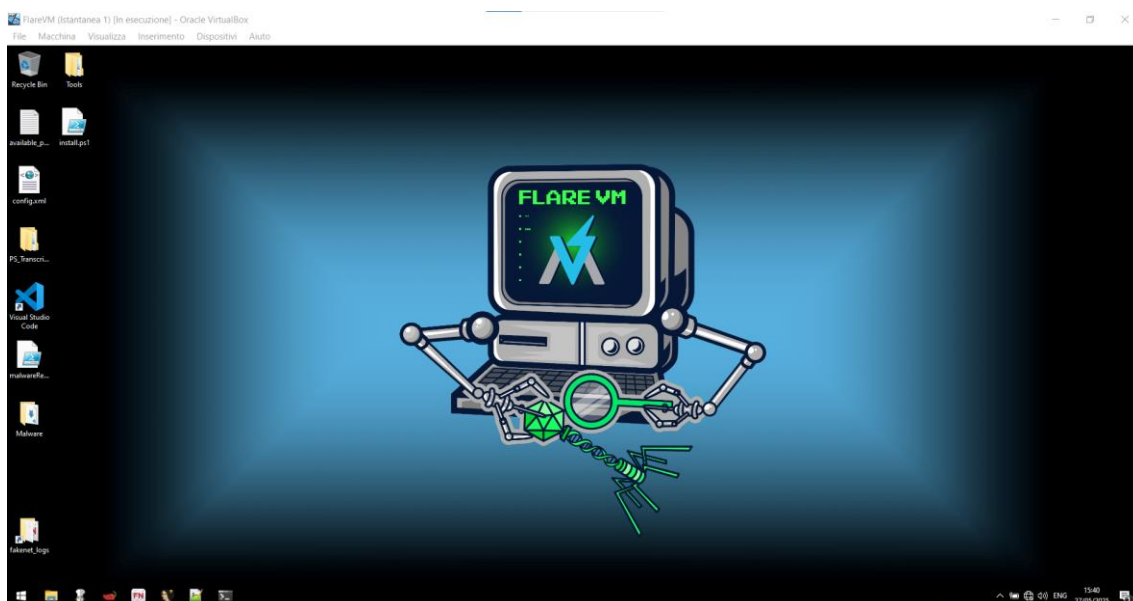
Creiamo un'icona sul desktop





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.