LABORATORIO 4 FEBBRAIO 2025 S9-L1

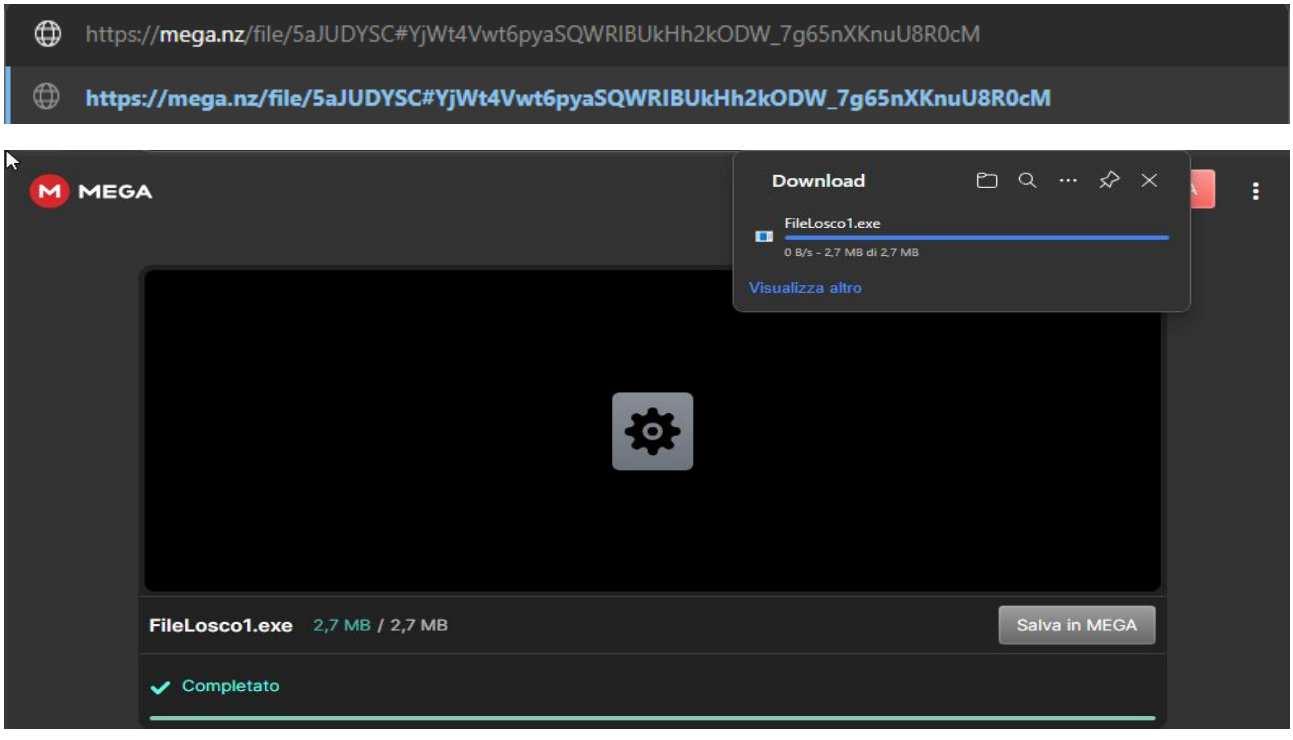
Attività di Analisi del Malware Oggetto: Sarà condiviso un malware relativamente innocuo.

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.

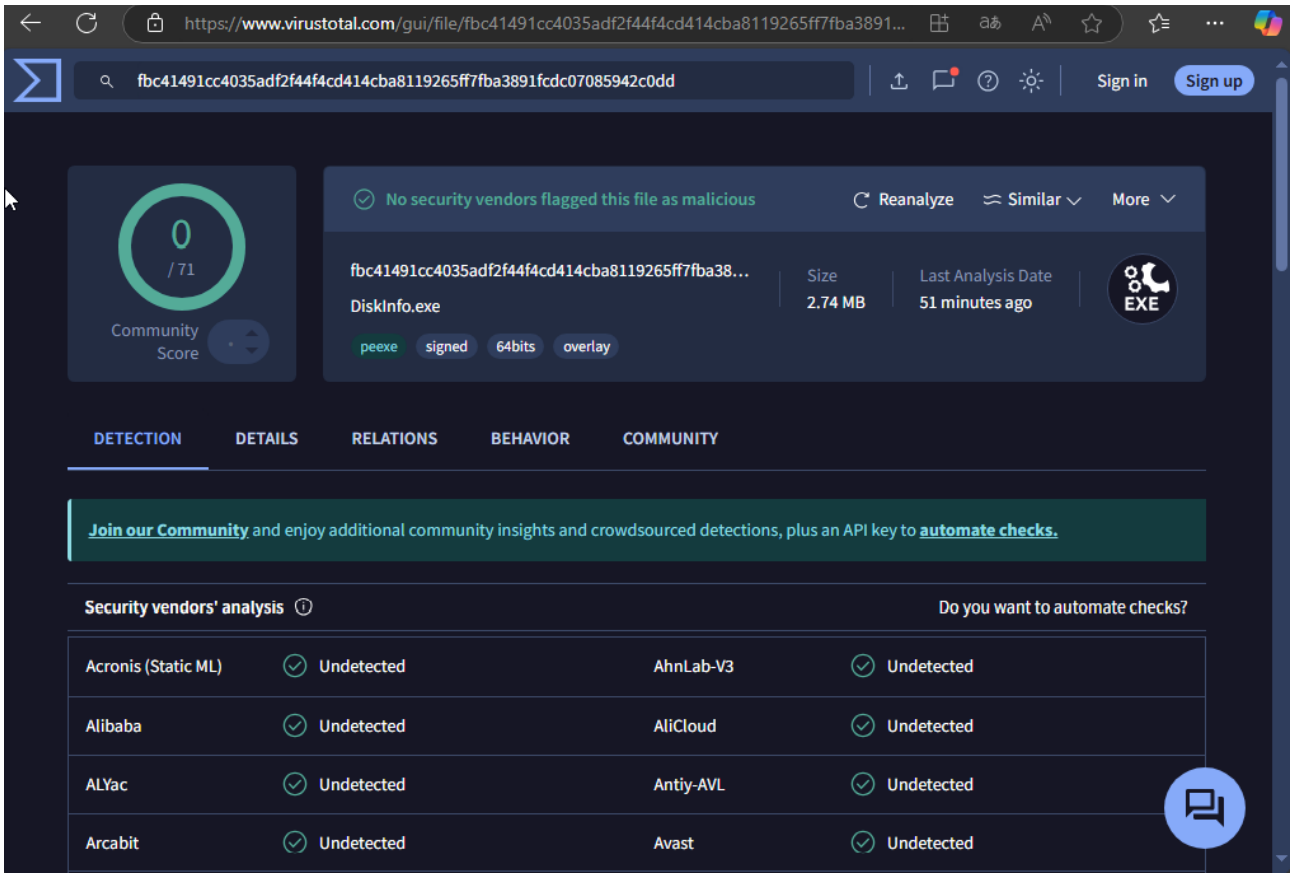
Avviamo la macchina virtuale Windows10 sulla quale scaricheremo il file fornitoci dal professore.



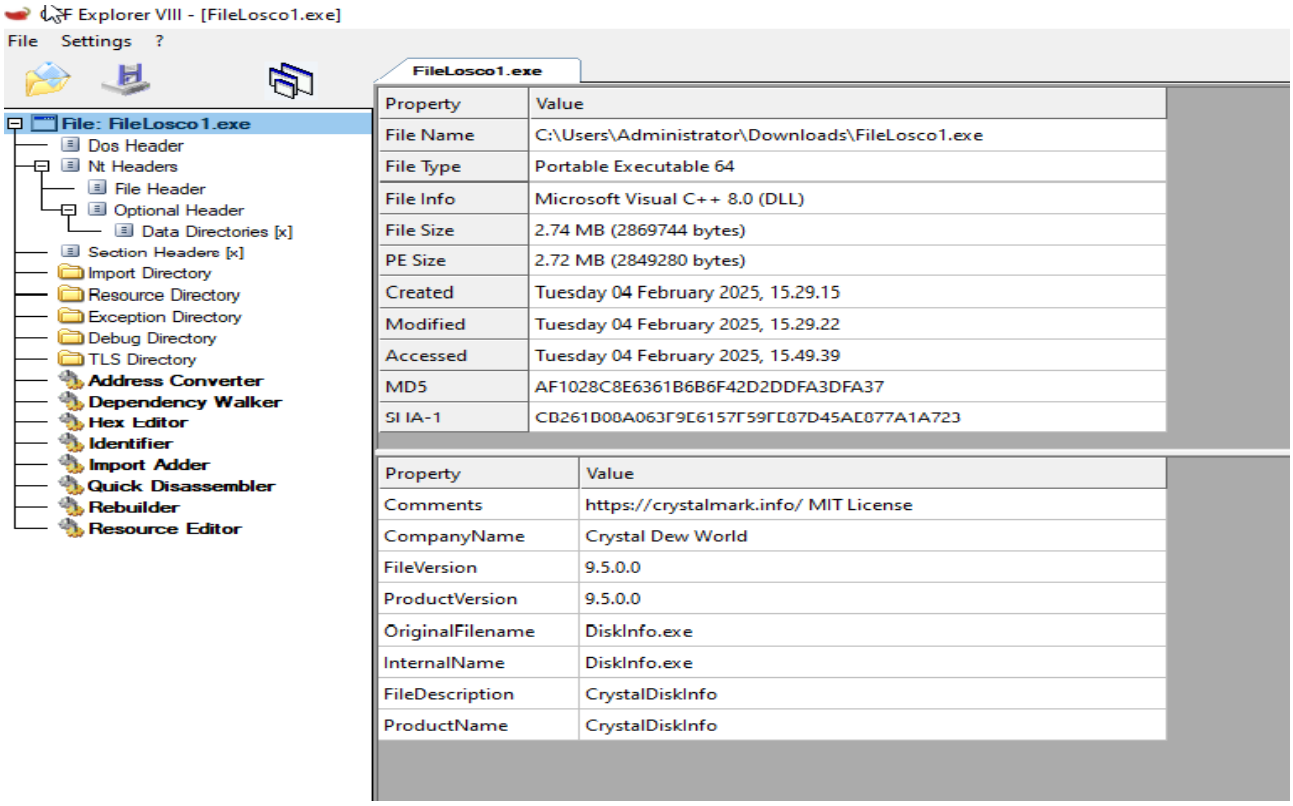
Una volta scaricato iniziamo ad analizzarlo coi i tool visti a lezione.

Dapprima effettuiamo una scansione con **virustotal** per controllare se il file sia malevolo o no.

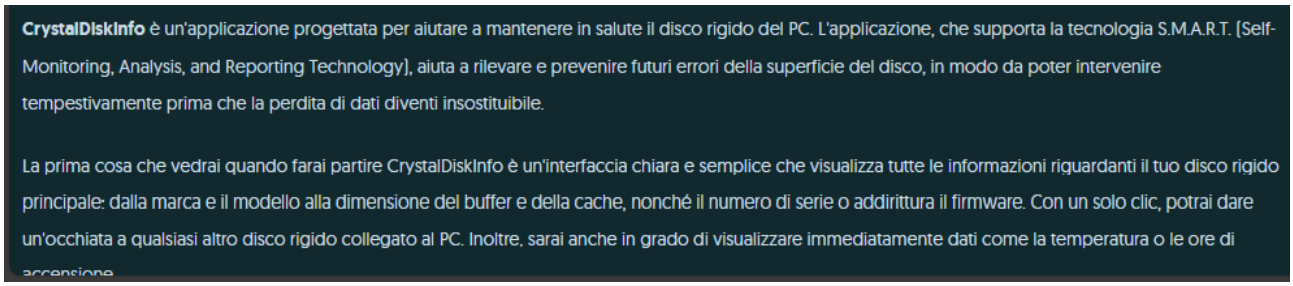
In questo caso il file è classificato come non malevolo dagli antivirus presenti nel tool.



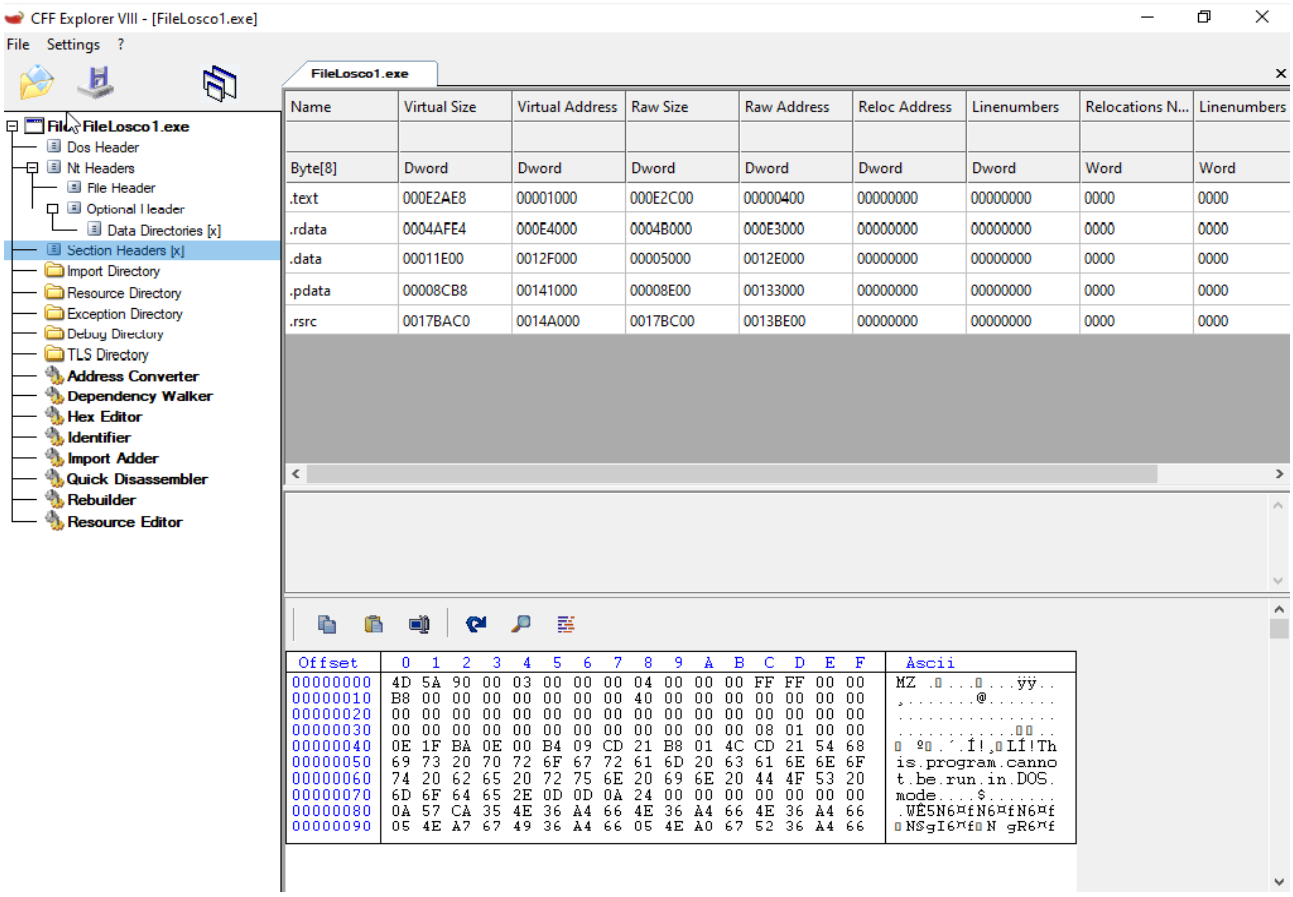
A questo punto procediamo con una analisi su CFF Explorer con il quale esamineremo il contenuto del file e la sua struttura.

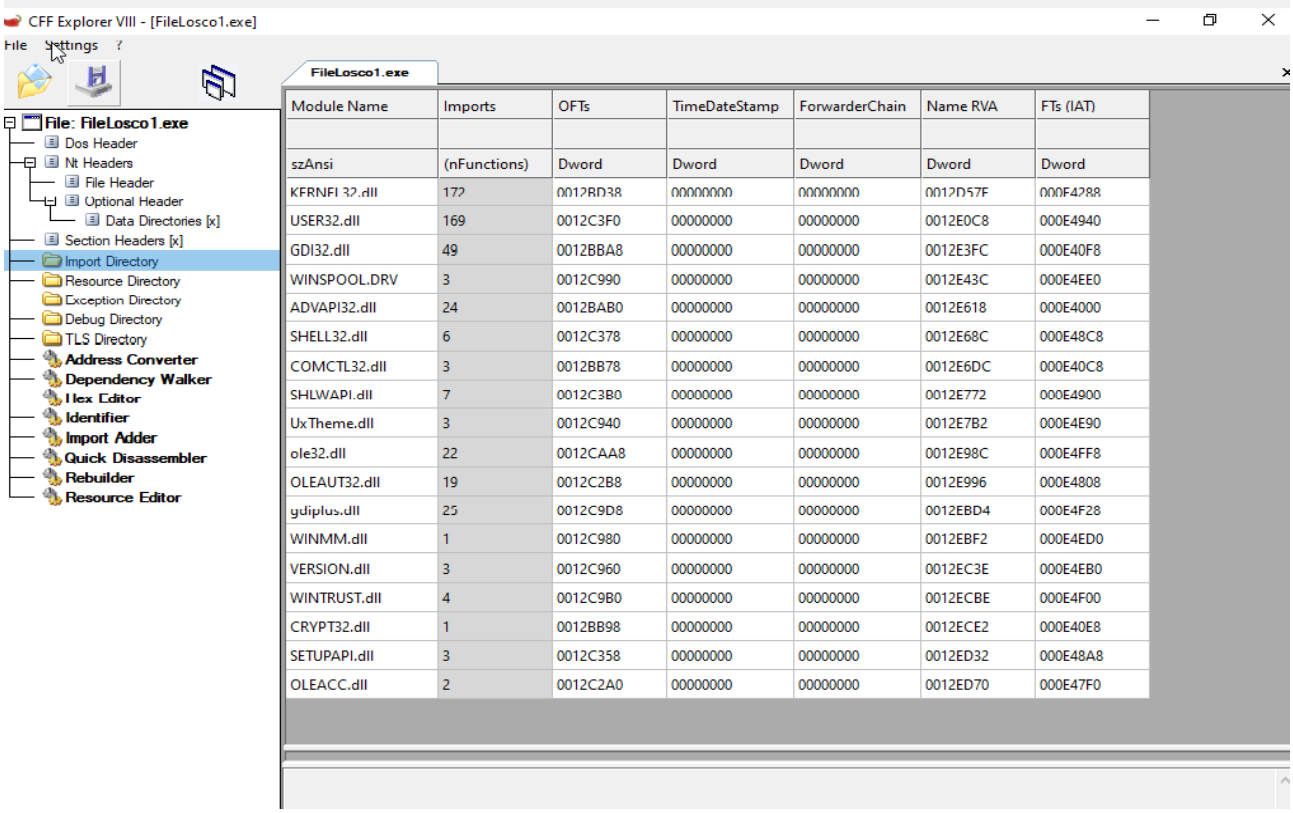


Dalle proprietà possiamo innanzitutto vedere che si tratta di un file al quale hanno cambiato il nome. Originariamente si chiamava DiskInfo.exe e facendo una ricerca è venuto fuori che si tratta di un file innocuo che serve a controllare lo stato del disco rigido del pc.

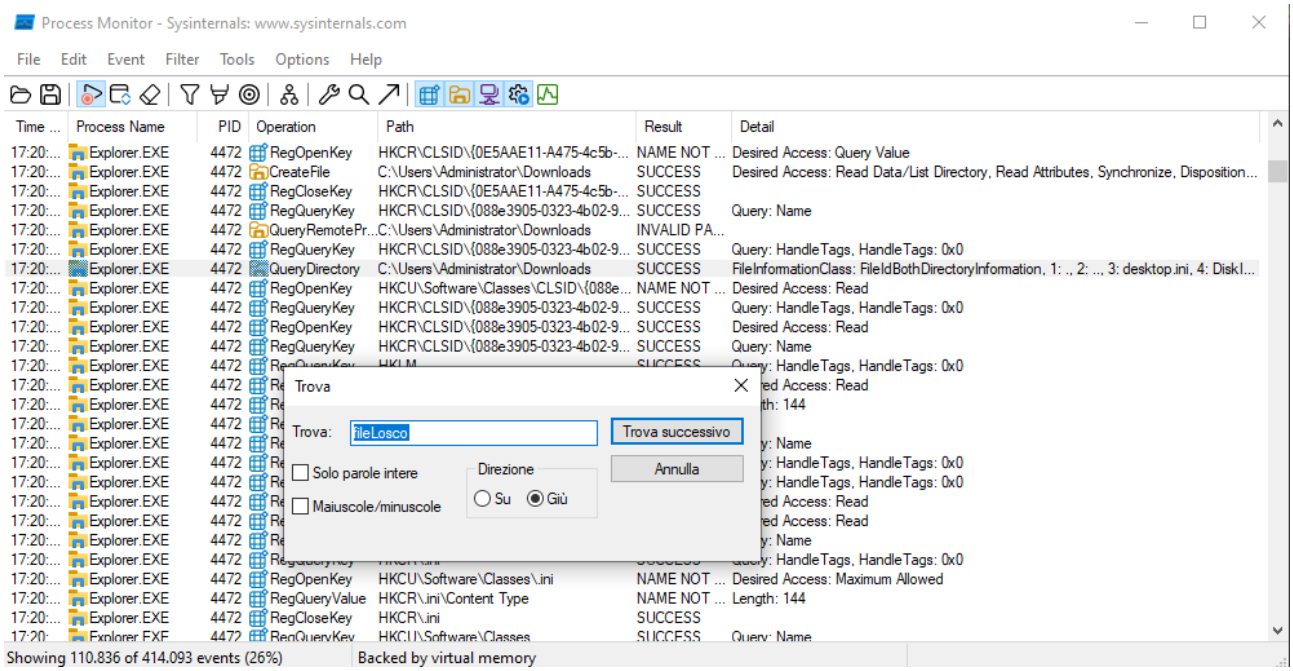


Proseguendo con la ricerca su CFF Explorer possiamo ottenere altre informazioni circa il contenuto del file come ad esempio gli headers e le directory importate.


CFF Explorer VIII - [FileLosco1.exe]
File Settings ?
FileLosco1.exe
File: FileLosco1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Exception Directory
Debug Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
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
.text | 000E2AE8 | 00001000 | 000E2C00 | 00000400 | 00000000 | 00000000 | 0000 | 0000
.rdata | 0004AFE4 | 000E4000 | 0004B000 | 000E3000 | 00000000 | 00000000 | 0000 | 0000
.data | 00011E00 | 0012F000 | 00005000 | 0012E000 | 00000000 | 00000000 | 0000 | 0000
.pdata | 00008CB8 | 00141000 | 00008E00 | 00133000 | 00000000 | 00000000 | 0000 | 0000
.rsrc | 0017BAC0 | 0014A000 | 0017BC00 | 0013BE00 | 00000000 | 00000000 | 0000 | 0000
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
00000010 B8 00 00 00 00 00 00 00 40 00 00 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 08 01 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 is.program.canno
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t.be.run.in.DOS.
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode....$.....
00000080 0A 57 CA 35 4E 36 A4 66 4E 36 A4 66 4E 36 A4 66
00000090 05 4E A7 67 49 36 A4 66 05 4E A0 67 52 36 A4 66


CFF Explorer VIII - [FileLosco1.exe]
File Settings ?
FileLosco1.exe
File: FileLosco1.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Exception Directory
Debug Directory
TLS Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword
KERNEL32.dll | 172 | 0012BD38 | 00000000 | 00000000 | 0012D57F | 000E4288
USER32.dll | 169 | 0012C3F0 | 00000000 | 00000000 | 0012E0C8 | 000E4940
GDI32.dll | 49 | 0012BBA8 | 00000000 | 00000000 | 0012E3FC | 000E40F8
WINSPOOL.DRV | 3 | 0012C990 | 00000000 | 00000000 | 0012E43C | 000E4EE0
ADVAPI32.dll | 24 | 0012BAB0 | 00000000 | 00000000 | 0012E618 | 000E4000
SHELL32.dll | 6 | 0012C378 | 00000000 | 00000000 | 0012E68C | 000E48C8
COMCTL32.dll | 3 | 0012BB78 | 00000000 | 00000000 | 0012E6DC | 000E40C8
SHLWAPI.dll | 7 | 0012C3B0 | 00000000 | 00000000 | 0012E772 | 000E4900
UxTheme.dll | 3 | 0012C940 | 00000000 | 00000000 | 0012E7B2 | 000E4E90
ole32.dll | 22 | 0012CAA8 | 00000000 | 00000000 | 0012E98C | 000E4FF8
OLEAUT32.dll | 19 | 0012C2B8 | 00000000 | 00000000 | 0012E996 | 000E4808
gdiplus.dll | 25 | 0012C9D8 | 00000000 | 00000000 | 0012EBD4 | 000E4F28
WINMM.dll | 1 | 0012C980 | 00000000 | 00000000 | 0012EBF2 | 000E4ED0
VERSION.dll | 3 | 0012C960 | 00000000 | 00000000 | 0012EC3E | 000E4EB0
WINTRUST.dll | 4 | 0012C9B0 | 00000000 | 00000000 | 0012ECBE | 000E4F00
CRYPT32.dll | 1 | 0012BB98 | 00000000 | 00000000 | 0012ECE2 | 000E40E8
SETUPAPI.dll | 3 | 0012C358 | 00000000 | 00000000 | 0012ED32 | 000E48A8
OLEACC.dll | 2 | 0012C2A0 | 00000000 | 00000000 | 0012ED70 | 000E47F0

A questo punto procediamo con l'esecuzione del file per osservare il suo comportamento. Utilizziamo Procrom64 e cerchiamo il file in questione.



Possiamo osservare l'orario delle attività, il process name, il PID, il tipo di operazione eseguita, il path dell'oggetto su cui l'operazione è stata eseguita, il risultato e i dettagli aggiuntivi.