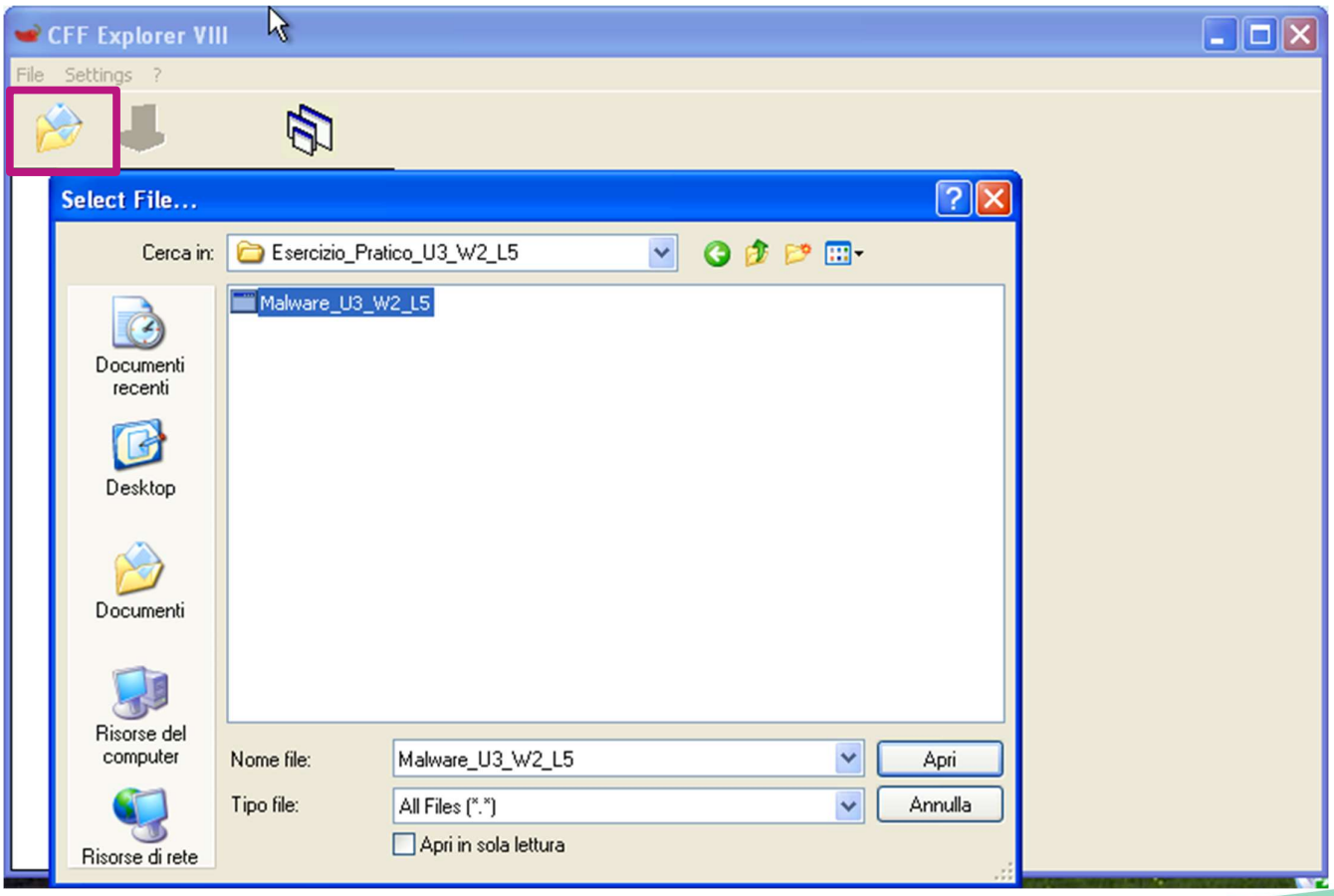
REPORT EPICODE

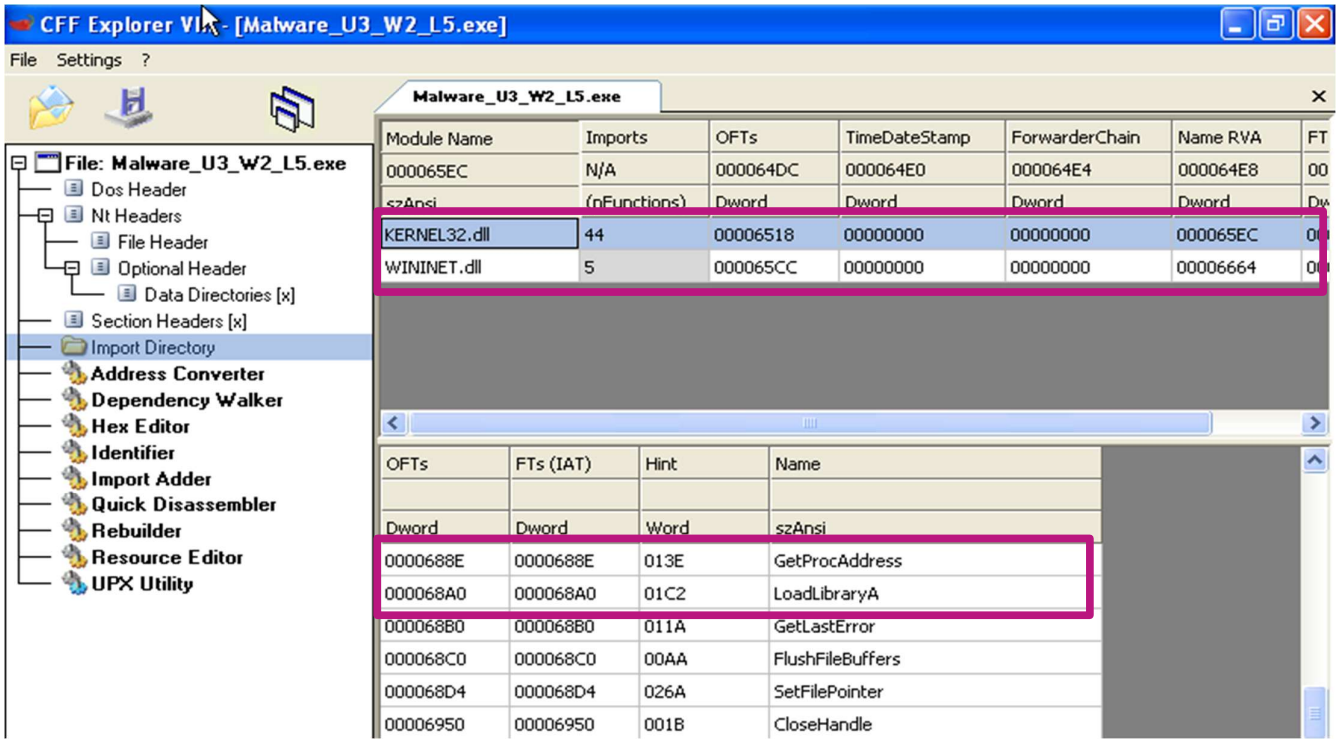
DATA
07/07/2023

Punto 1: individuare librerie importate e sezioni di cui si compone il file Malware_U3_W2_L5

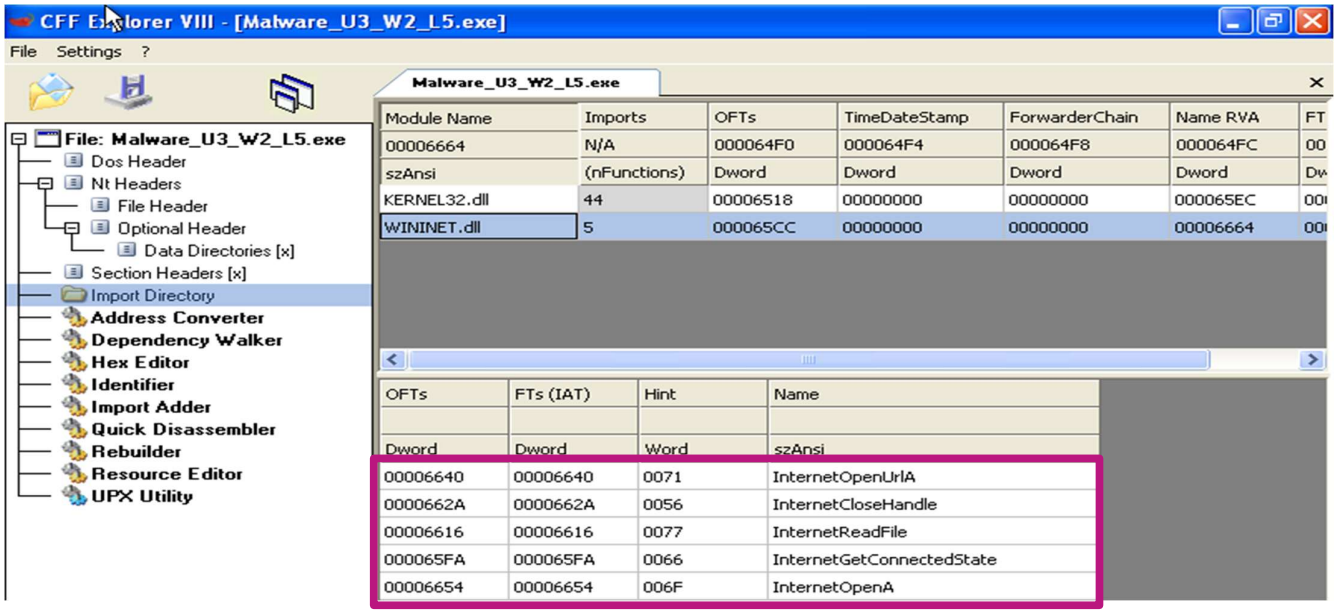
Per lo svolgimento dell'esercizio ho scelto di usare il programma **CFF Explorer** che permette di controllare le librerie e le funzioni importate, se non anche le sezioni di cui si compone il software, operazione fondamentale per capire lo scopo del malware.
Ho quindi avviato il programma e scelto il file eseguibile, come da consegna, dopo aver cliccato sull'icona a forma di cartella.



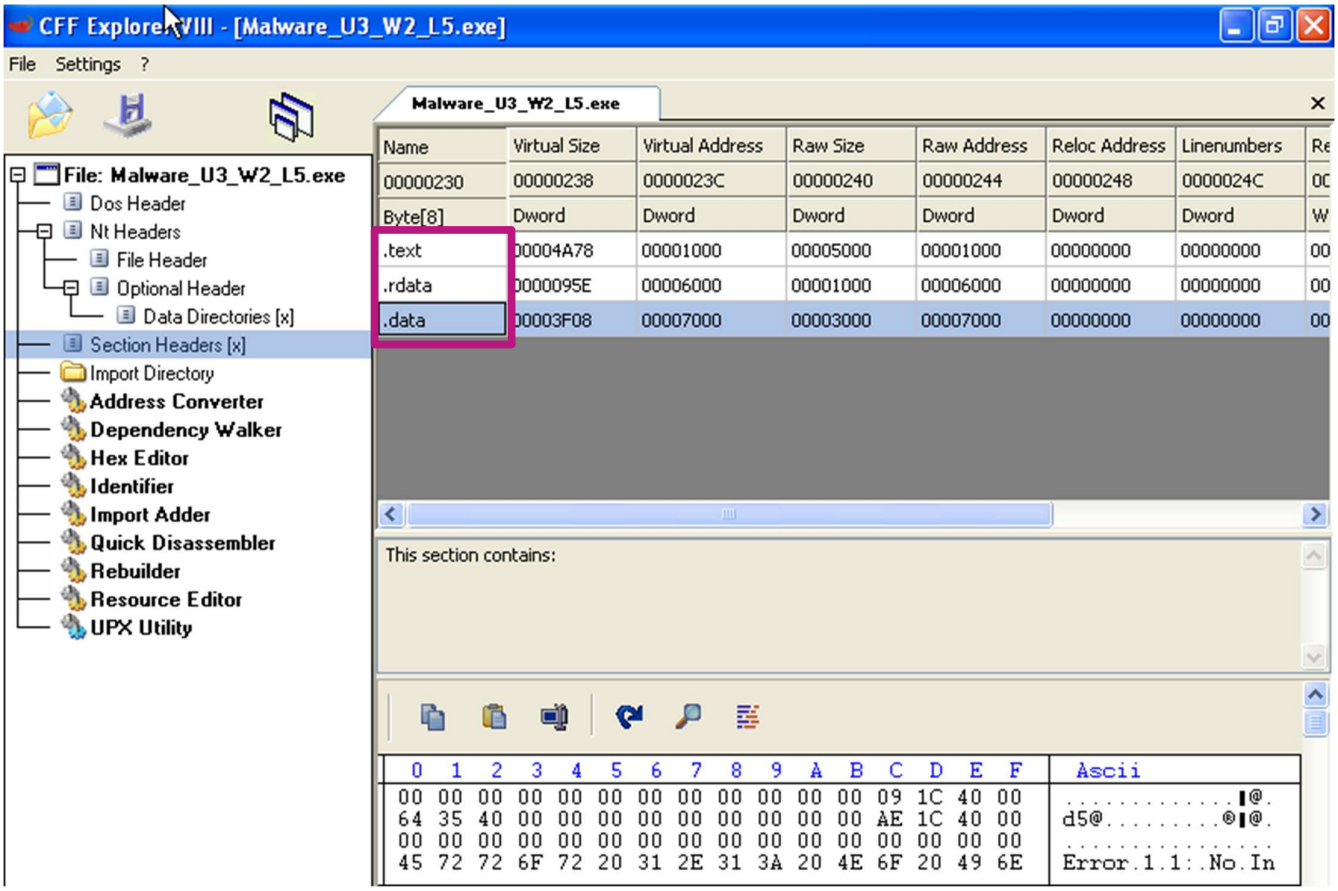
Cliccando su import directory ho trovato le librerie importate:



- **KERNEL32.dll:** libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo come, per esempio, manipolazione dei file o la gestione della memoria. Sembra che il malware utilizzi il caricamento della libreria durante l'esecuzione; infatti, figurano le funzioni **LoadLibraryA** e **GetProcAddress** le quali vengono utilizzate per caricare funzioni addizionali durante l'esecuzione.
- **WININET.dll:** libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP. Infatti, nell'immagine sottostante possiamo notare le funzioni:

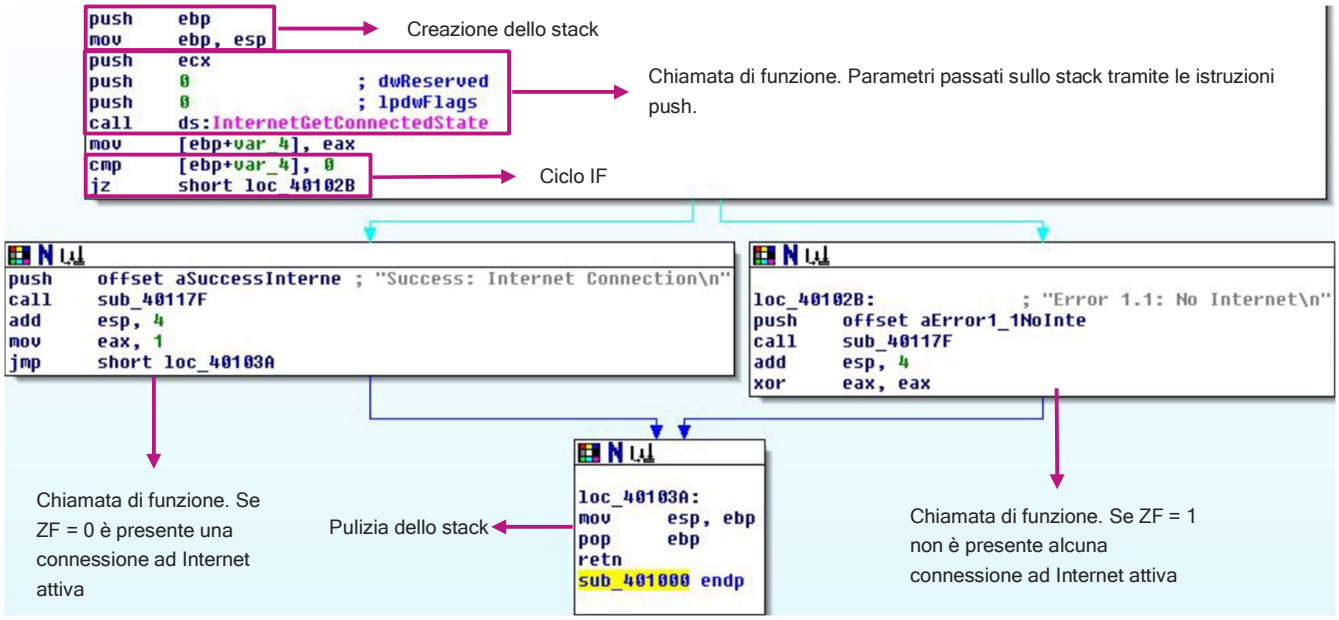


Cliccando su **Section Headers** ho trovato le sezioni di cui è composto il malware:



- **.text:** contiene le istruzioni che la CPU eseguirà una volta avviato il malware. Questa è l'unica sezione di un file **.exe** eseguita dalla CPU, poiché le altre sezioni contengono dati o informazioni di supporto.
- **.rdata:** include le informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile.
- **.data:** contiene i dati e le variabili globali del programma eseguibile. Essendo variabili globali sono accessibili da tutte le funzioni del programma.

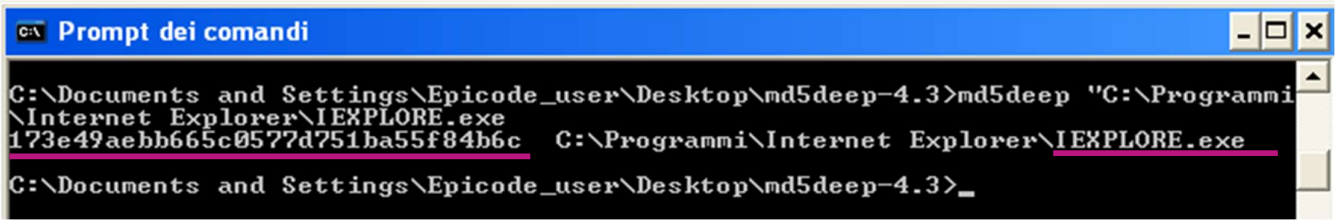
Punto 2: identificare i costrutti ed ipotizzare il comportamento della funzionalità del codice in Assembly



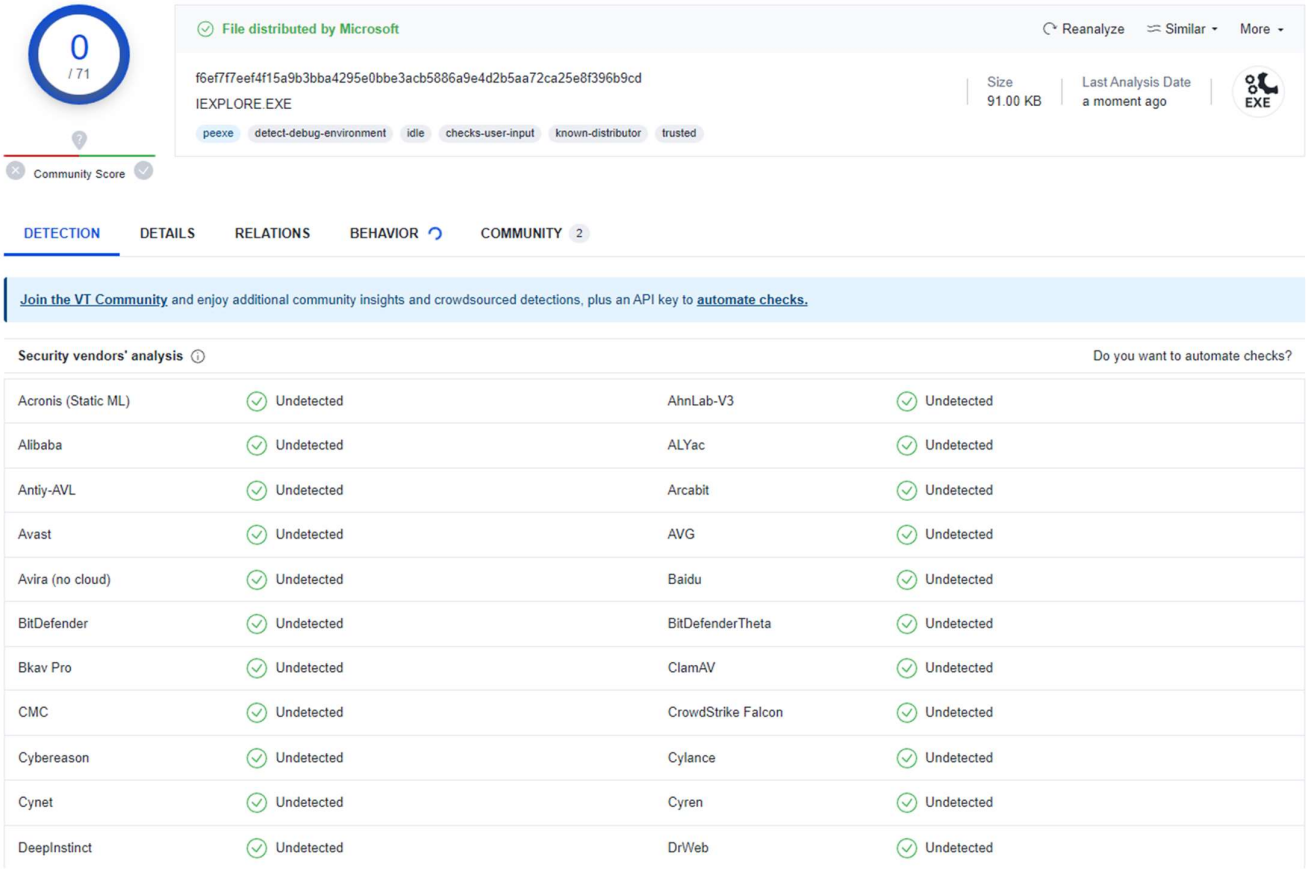
Ipotesi di comportamento: il malware cerca di recuperare lo stato di connessione di un sistema chiamando la funzione **InternetGetConnectedState**. Se la condizione del ciclo IF risulta **vera**, quindi la variabile =/= 0, è presente una connessione ad Internet attiva. Al contrario, non è presente nessuna connessione ad Internet attiva e la funzione restituirà errore.
Infatti, nel ciclo if, viene effettuata la comparazione tra la variabile e 0, successivamente con **jz** = jump zero, si salta in una locazione della memoria nel caso in cui ZF = 1, ovvero nel caso in cui la condizione sia **falsa.**
Infine, quando la funzione chiamata finisce il suo compito, verrà eliminato il suo stack e le sue variabili locali, le quali non più necessarie per riportare l'esecuzione alla funzione chiamante, ovvero la **pulizia dello stack.**

BONUS: convincere il dipendente che il file IEXPLORE.EXE non è maligno.

Inizio con un'analisi statica del file.
Per prima cosa recupero l'hash del file eseguibile IEXPLORE.exe con l'utility **md5deep.**



Ho cercato l'hash online per confermare non fosse un malware e trovare informazioni sul comportamento del file. Ho utilizzato il sito web Virus Total, su cui non stati rilevati malware.



Possiamo osservare i vari nomi usati per nominare il file e il copyright. Il file IEXPLORE.exe appartiene a Microsoft.

Names

iexplore
IEXPLORE.EXE
iexplore.exe
iexplore.e_e
AAA2F14500FAC0E66C3701CE010A60003E8CA866.exe
file-1066147_old

Signature info

Signature Verification

File is not signed

File Version Information

Copyright	© Microsoft Corporation. Tutti i diritti riservati.
Product	Sistema operativo Microsoft® Windows®
Description	Internet Explorer
Original Name	IEXPLORE.EXE
Internal Name	iexplore
File Version	6.00.2900.5512 (xpsp.080413-2105)

Known Source

Organization	Microsoft Corporation
File name	iexplore.exe
Description	The file belongs to the Windows XP Home N Refurbisher product, it can be found, for example, in SW CD Win XP Home N Refurbisher Italian #1 ProdAct SP3R OEM.

Vediamo le sezioni di cui si compone il file e le librerie importate ed esportate che corrispondono al file caricato su **CFF Explorer.**

Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	7579	7680	6.2	75b4ae57db4a0b8330a969a73170271e	77682.25
.data	12288	156	512	2.57	3250ebd1e3513e9aa0c55ad75a9f41c3	70657
.rsrc	16384	83760	83968	5.69	62816de28514b1c76f2822cc8250e772	2216213.5

Imports

+ SHDOCVW.dll
+ KERNEL32.dll
+ msvcrt.dll
+ SHLWAPI.dll
+ USER32.dll

Exports

DllGetLCID

Ho verificato di nuovo le sezioni e le librerie importate dal file IEXPLORE.exe usando il tool **CFF Explorer.**

CFF Explorer VIII - [IEXPLORE.EXE]

File Settings ?

Malware_U3_W2_L5.exe | IEXPLORE.EXE

File: IEXPLORE.EXE
- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Export Directory
- Import Directory
- Resource Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Re
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	W
.text	00001D9B	00001000	00001E00	00000400	00000000	00000000	00
.data	0000009C	00003000	00000200	00002200	00000000	00000000	00
.rsrc	00014730	00004000	00014800	00002400	00000000	00000000	00

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	E8	00	00	00	.....

CFF Explorer VIII - [IEXPLORE.EXE]

File Settings ?

Malware_U3_W2_L5.exe | IEXPLORE.EXE

File: IEXPLORE.EXE
- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Export Directory
- Import Directory
- Resource Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

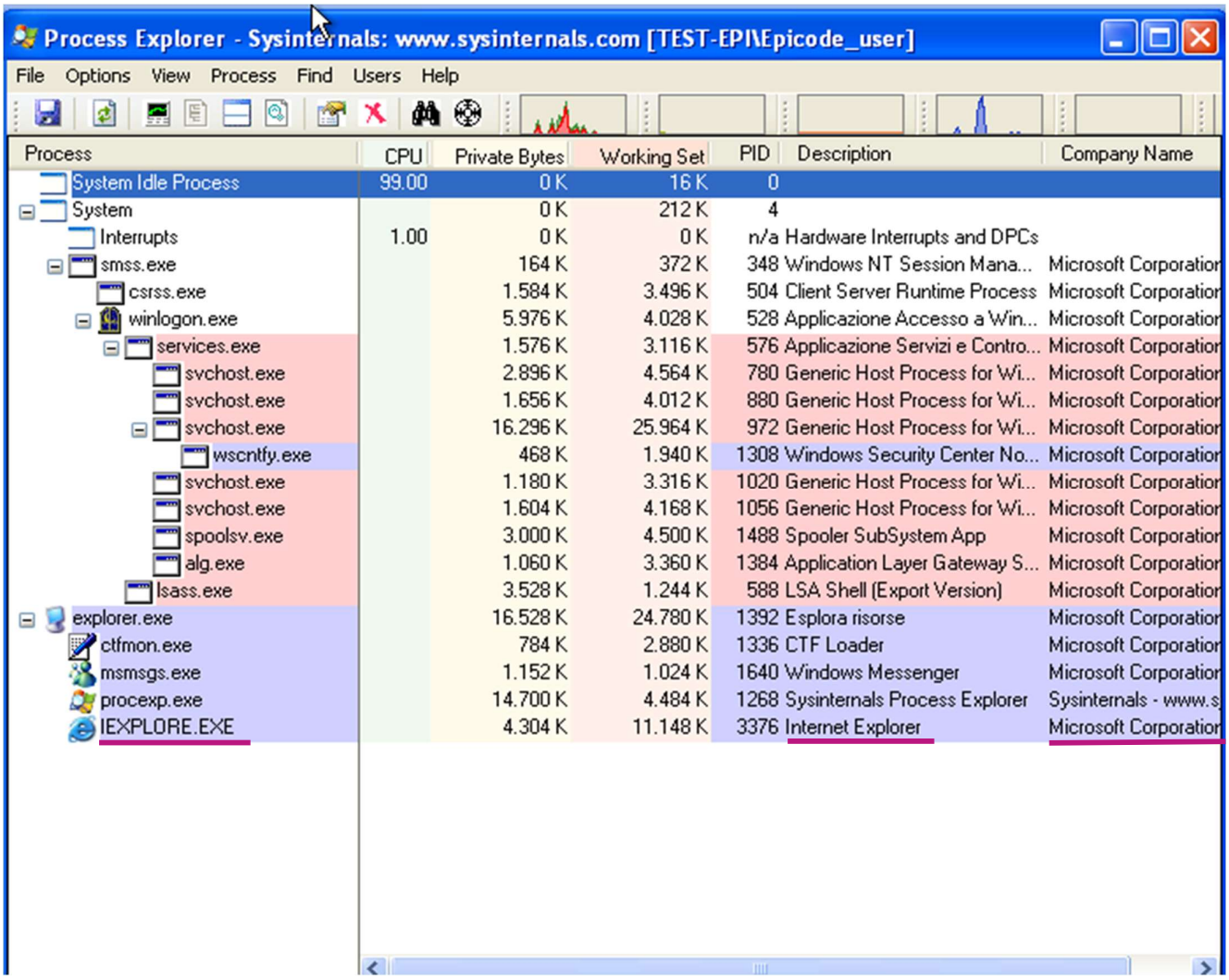
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FT
00001C4C	N/A	00001A74	00001A78	00001A7C	00001A80	00
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dw
msvcrt.dll	1	00002830	FFFFFFFF	FFFFFFFF	0000284C	00
KERNEL32.dll	43	000026EC	FFFFFFFF	FFFFFFFF	00002B66	00
USER32.dll	16	000027EC	FFFFFFFF	FFFFFFFF	00002C8C	00
SHLWAPI.dll	16	000027A8	FFFFFFFF	FFFFFFFF	00002D30	00
SHDOCVW.dll	2	0000279C	FFFFFFFF	FFFFFFFF	00002D3C	00

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00002838	4DC65C94	00ED	_except_handler3

Per l'analisi dinamica del file IEXPLORE.exe ho eseguito il file in ambiente dedicato ed utilizzato i seguenti tool secondo il seguente ordine:

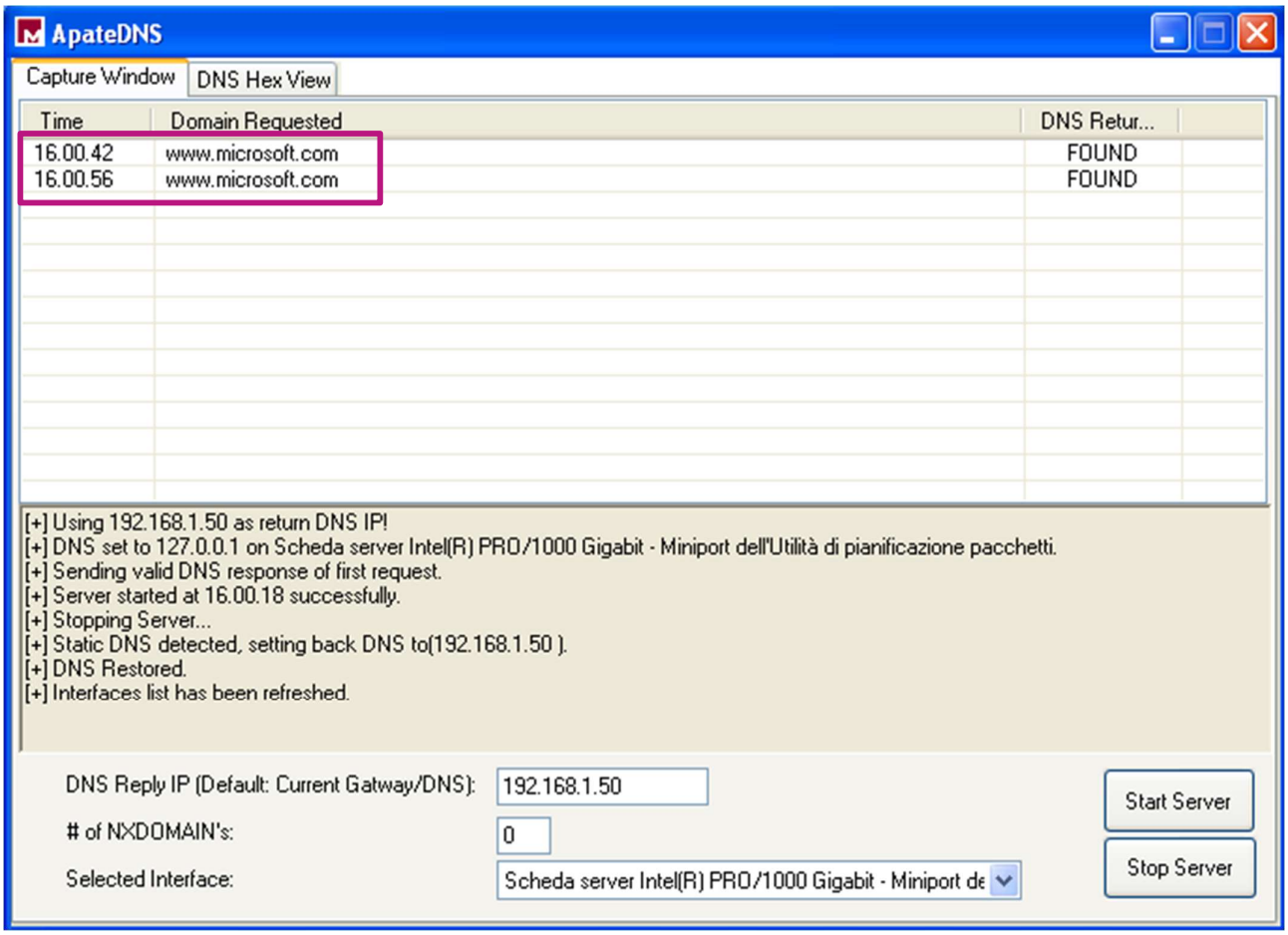
- **Process Explorer**
- **ApateDNS**
- **RegShot**
- **Procmon**

Process Explorer è un tool che permette l'analisi dettagliata di tutti i processi in esecuzione su un sistema. Una volta avviato IEXPLORE.exe ho ottenuto il seguente risultato: come possiamo vedere dalla Description si tratta di Internet Explorer appartenente al Company Name Microsoft Corporation. Non ho notato cambiamenti subiti nel pannello dei processi durante l'esecuzione del file.

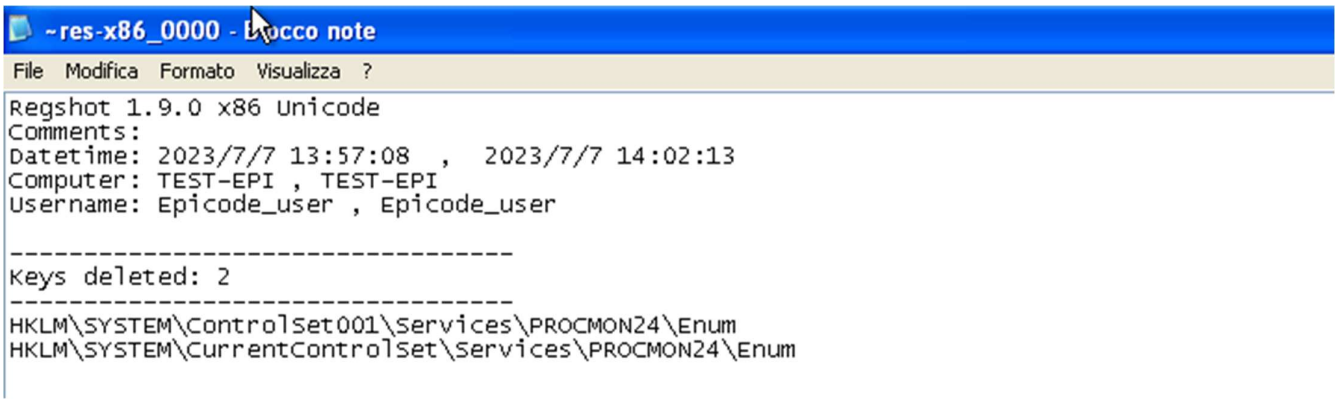


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	99.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	1.00	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	348	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1.584 K	3.496 K	504	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		5.976 K	4.028 K	528	Applicazione Accesso a Win...	Microsoft Corporation
services.exe		1.576 K	3.116 K	576	Applicazione Servizi e Contro...	Microsoft Corporation
svchost.exe		2.896 K	4.564 K	780	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.656 K	4.012 K	880	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		16.296 K	25.964 K	972	Generic Host Process for Wi...	Microsoft Corporation
wscntfy.exe		468 K	1.940 K	1308	Windows Security Center No...	Microsoft Corporation
svchost.exe		1.180 K	3.316 K	1020	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe		1.604 K	4.168 K	1056	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe		3.000 K	4.500 K	1488	Spooler SubSystem App	Microsoft Corporation
alg.exe		1.060 K	3.360 K	1384	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3.528 K	1.244 K	588	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		16.528 K	24.780 K	1392	Esplora risorse	Microsoft Corporation
ctfmon.exe		784 K	2.880 K	1336	CTF Loader	Microsoft Corporation
msmsgs.exe		1.152 K	1.024 K	1640	Windows Messenger	Microsoft Corporation
procexp.exe		14.700 K	4.484 K	1268	Sysinternals Process Explorer	Sysinternals - www.s
IEXPLORE.EXE		4.304 K	11.148 K	3376	Internet Explorer	Microsoft Corporation

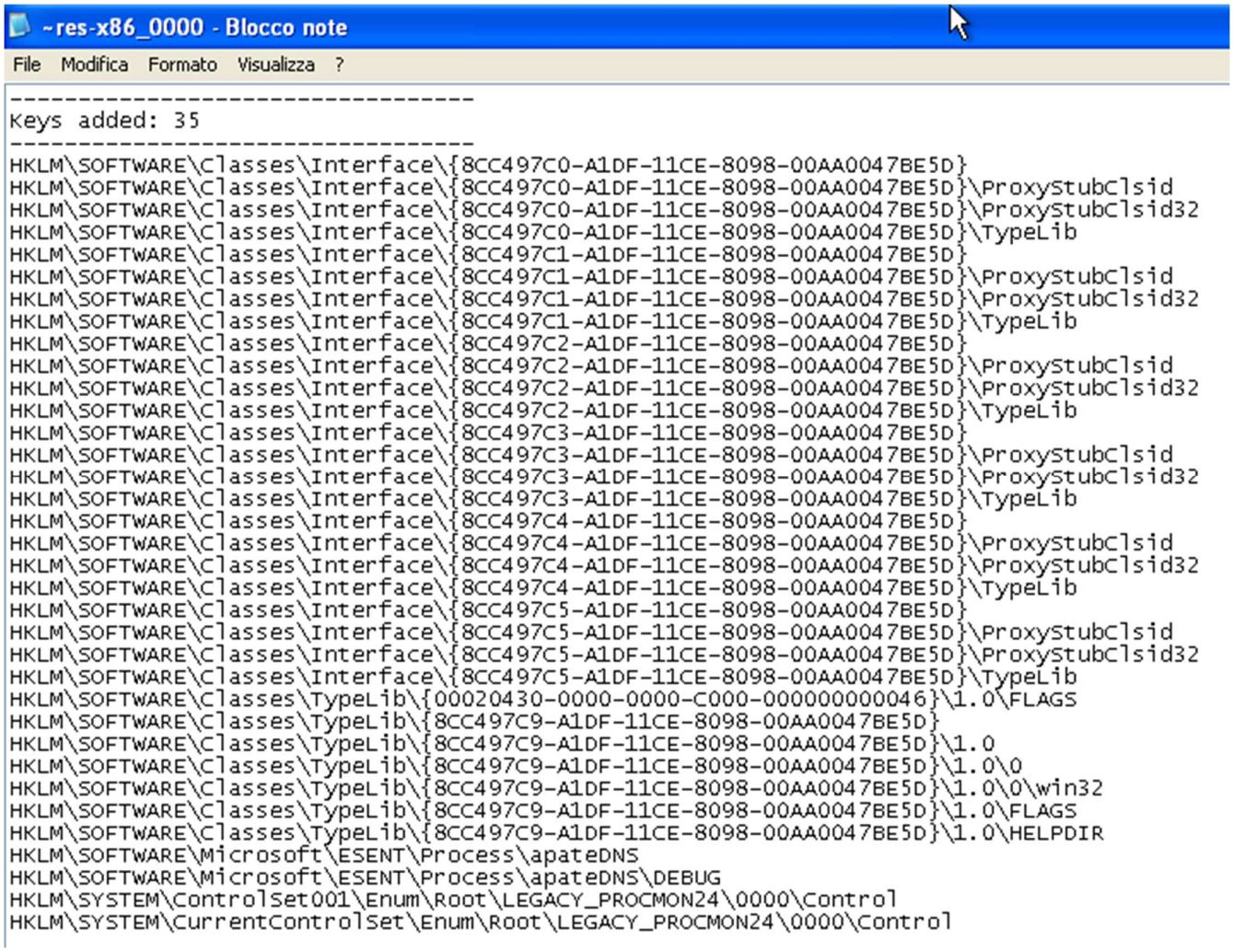
ApateDns è stato utilizzato per la simulazione di un server DNS per intercettare tutte le richieste effettuate dal file verso i domini Internet. Gli unici domini a cui sono state effettuate le richieste appartengono a Microsoft.



RegShot permette di paragonare due istantanee delle chiavi di registro, una istantanea è stata catturata prima dell'esecuzione del file, la seconda istantanea successivamente l'esecuzione del file e sono state messe a confronto. Le uniche chiavi di registro cancellate ed aggiunte sono le **HKEY LOCAL MACHINE**, le quali includono le impostazioni comuni per tutti gli utenti di sistema.



La sottochiave SOFTWARE può essere la chiave del Registro di sistema a cui gli utenti accedono più comunemente. Memorizza le informazioni di configurazione di vari programmi installati sul computer. Quando viene installato un programma, scriverà i dati nella chiave di registro SOFTWARE per memorizzare le impostazioni dell'applicazione. La prossima volta che verrà aperta l'applicazione, le sue impostazioni specifiche verranno caricate automaticamente nella memoria del computer. In questo modo, non è necessario configurare il programma ogni volta che lo si utilizza.



~res-x86_0000 - Blocco note

File Modifica Formato Visualizza ?

```
----------------------------------
Keys added: 35
----------------------------------
HKLM\SOFTWARE\Classes\Interface\{8CC497C0-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C0-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C0-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C0-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\Interface\{8CC497C1-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C1-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C1-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C1-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\Interface\{8CC497C2-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C2-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C2-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C2-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\Interface\{8CC497C3-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C3-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C3-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C3-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\Interface\{8CC497C4-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C4-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C4-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C4-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\Interface\{8CC497C5-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\Interface\{8CC497C5-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid
HKLM\SOFTWARE\Classes\Interface\{8CC497C5-A1DF-11CE-8098-00AA0047BE5D}\ProxyStubClsid32
HKLM\SOFTWARE\Classes\Interface\{8CC497C5-A1DF-11CE-8098-00AA0047BE5D}\TypeLib
HKLM\SOFTWARE\Classes\TypeLib\{00020430-0000-0000-C000-000000000046}\1.0\FLAGS
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}\1.0
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}\1.0\0
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}\1.0\0\win32
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}\1.0\FLAGS
HKLM\SOFTWARE\Classes\TypeLib\{8CC497C9-A1DF-11CE-8098-00AA0047BE5D}\1.0\HELPDIR
HKLM\SOFTWARE\Microsoft\ESENT\Process\apateDNS
HKLM\SOFTWARE\Microsoft\ESENT\Process\apateDNS\DEBUG
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON24\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON24\0000\Control
```

Process Monitor, abbreviato Procmon permette di monitorare i processi e i thread attivi, l'attività di rete, l'accesso ai file ecc.

Qui lo screen delle attività relative al file system.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path
16.00....	Explorer.EXE	1392	CloseFile	C:\WINDOWS\system32\winscard.dll
16.00....	Explorer.EXE	1392	ReadFile	C:\WINDOWS\system32\shell32.dll
16.00....	Explorer.EXE	1392	ReadFile	C:\WINDOWS\system32\advapi32.dll
16.00....	Explorer.EXE	1392	CreateFile	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFileMapping	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFileMapping	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	QueryBasicInformationFile	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	QueryStandardInformatio...	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	QueryNameInformationFile	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	QueryOpen	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFile	C:\Programmi\Internet Explorer
16.00....	Explorer.EXE	1392	QueryDirectory	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CloseFile	C:\Programmi\Internet Explorer
16.00....	Explorer.EXE	1392	QueryStandardInformatio...	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFileMapping	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	QueryStandardInformatio...	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFileMapping	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	CreateFile	C:\Programmi\Internet Explorer\IEXPLORE.EXE.Manifest
16.00....	Explorer.EXE	1392	QueryOpen	C:\Programmi\Internet Explorer
16.00....	Explorer.EXE	1392	CloseFile	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG
16.00....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG
16.00....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG
16.00....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG
16.00....	Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shdocvw.dll
16.00....	Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shdocvw.dll
16.00....	Explorer.EXE	1392	QueryOpen	C:\WINDOWS\system32\shdocvw.dll
16.01....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG
16.01....	Explorer.EXE	1392	SetEndOfFileInformation...	C:\Documents and Settings\Epicode_user\ntuser.dat.LOG

In questo screen vengono visualizzate le attività relative ai processi e thread:

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path
15.59....	Explorer.EXE	1392	Thread Create	
15.59....	Explorer.EXE	1392	Thread Exit	
15.59....	Explorer.EXE	1392	Thread Exit	
15.59....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\shgina.dll
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\msgina.dll
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\odbc32.dll
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\comdlg32.dll
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\odbcint.dll
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Process Create	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\sxs.dll
16.00....	Explorer.EXE	1392	Thread Create	
16.00....	Explorer.EXE	1392	Load Image	C:\WINDOWS\system32\winscard.dll
16.00....	Explorer.EXE	1392	Thread Exit	
16.00....	Explorer.EXE	1392	Process Create	C:\Programmi\Internet Explorer\IEXPLORE.EXE
16.01....	Explorer.EXE	1392	Thread Exit	
16.01....	Explorer.EXE	1392	Thread Exit	
16.01....	Explorer.EXE	1392	Thread Create	

In questo screen osserviamo le attività relative ai registri di Windows.

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path
16.01....	Explorer.EXE	1392	RegQueryKey	HKCU\Software\Classes
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegOpenKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegQueryKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegQueryValue	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder\WantsFORDISPLA
16.01....	Explorer.EXE	1392	RegCloseKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7007ACC7-3202-11D1-
16.01....	Explorer.EXE	1392	RegQueryKey	HKCU\Software\Classes
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegOpenKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegQueryKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegQueryValue	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder\HideFolderVerbs
16.01....	Explorer.EXE	1392	RegCloseKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\ShellFolder
16.01....	Explorer.EXE	1392	RegQueryKey	HKCU\Software\Classes
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegOpenKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegQueryKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegOpenKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegCloseKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegQueryKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
16.01....	Explorer.EXE	1392	RegQueryValue	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\LocalizedString
16.01....	Explorer.EXE	1392	RegOpenKey	HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
16.01....	Explorer.EXE	1392	RegQueryValue	HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache\@C:\WINDOWS\system32\n
16.01....	Explorer.EXE	1392	RegCloseKey	HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache
16.01....	Explorer.EXE	1392	RegCloseKey	HKCR\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}