Internet Explorer e’ un malware?

Analisi Statica del File iexplore.exe:

- **Librerie Importate**:
  - ADVAPI32.dll: 13 funzioni
  - KERNEL32.dll: 56 funzioni
  - USER32.dll: 9 funzioni
  - msvcrt.dll: 29 funzioni
  - ntdll.dll: 3 funzioni

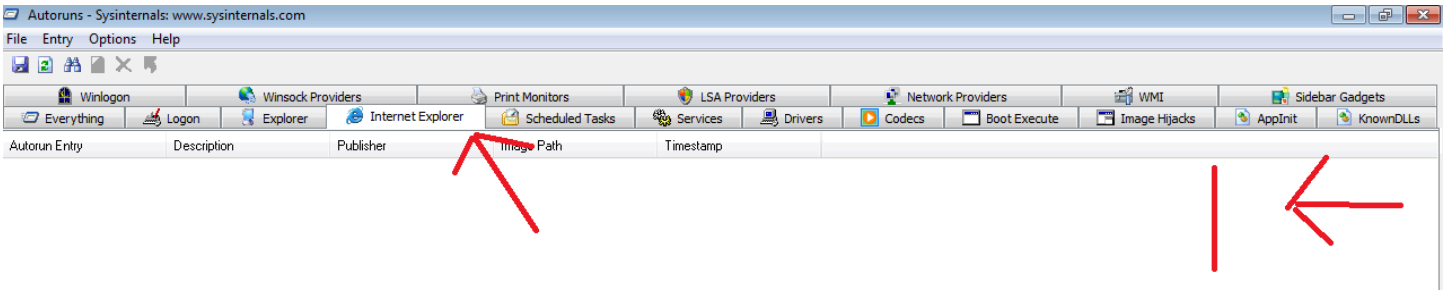
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFFFF	FFFFFFFF	0000F6A8	00009000
KERNEL32.dll	56	0000F728	FFFFFFFF	FFFFFFFF	0000F698	00009070
USER32.dll	9	0000F8F0	FFFFFFFF	FFFFFFFF	0000F68C	00009238
msvcrt.dll	29	0000F940	FFFFFFFF	FFFFFFFF	0000F680	00009288
ntdll.dll	3	0000FA30	FFFFFFFF	FFFFFFFF	0000F674	00009378

- **Sezioni del File**:
  - .text: Codice eseguibile
  - .rdata: Dati in sola lettura
  - .data: Dati leggibili e scrivibili
  - .pdata: Tabelle di dati del programma
  - .rsrc: Risorse (es: immagini)
  - .reloc: Tabelle di rilocazione

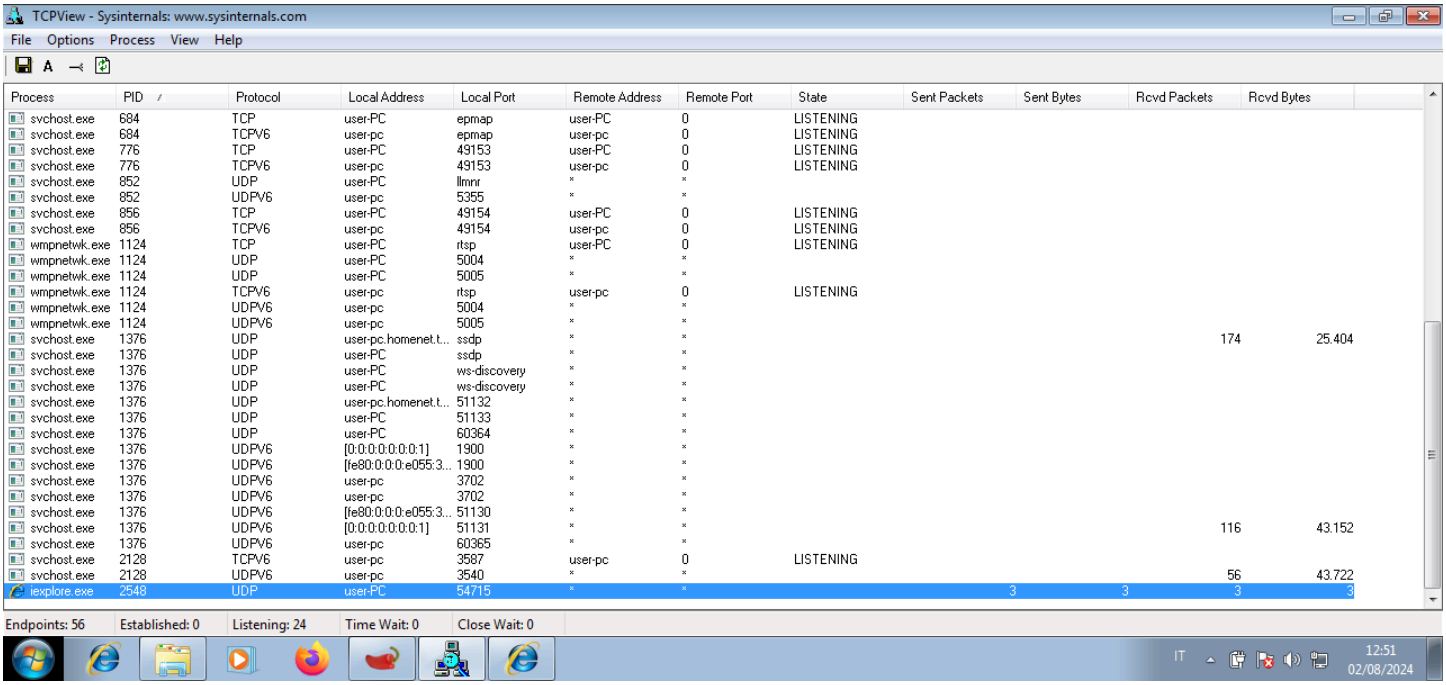
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00007349	00001000	00007400	00000400	00000000	00000000	0000	0000	60000020
.rdata	00007C08	00009000	00007E00	00007800	00000000	00000000	0000	0000	40000040
.data	00000B0C	00011000	00000A00	0000F600	00000000	00000000	0000	0000	C0000040
.pdata	00000564	00012000	00000600	00010000	00000000	00000000	0000	0000	40000040
.rsrc	00097020	00013000	00097200	00010600	00000000	00000000	0000	0000	40000040
.reloc	00000674	000AB000	00000800	000A7800	00000000	00000000	0000	0000	42000040

Analisi Dinamica del File iexplore.exe

- **Autoruns**:
  - Nessuna voce sospetta relativa a iexplore.exe.



- **TcpView**:
  - Connessioni di rete attive per iexplore.exe:
    - Nessuna connessione sospetta rilevata.
    - Il processo è attualmente in stato di ascolto (listening) su diverse porte, ma non ha stabilito connessioni attive.



Inoltre un file come iexplore.exe, dovrebbe avere una firma digitale valida di Microsoft. La firma digitale garantisce che il file non sia stato alterato e provenga da una fonte affidabile:

Property	Value
File Name	C:\Program Files\Internet Explorer\iexplore.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	678.77 KB (695056 bytes)
PE Size	672.00 KB (688128 bytes)
Created	Sunday 21 November 2010, 05.24.43
Modified	Sunday 21 November 2010, 05.24.43
Accessed	Sunday 21 November 2010, 05.24.43
MD5	86257731DDB311FBC283534CC0091634
SHA-1	2AA859F008FAFBAEFB578019ED0D65CD0933981C

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Internet Explorer
FileVersion	8.00.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	iexplore
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	IEXPLORE.EXE
ProductName	Windows® Internet Explorer

Possiamo notare che un malware potrebbe essere molto simile su certi aspetti, ma ricordiamoci che il fatto di non avere file sospetti su Autoruns è significativo. Questo dimostra che il file non ha intenzione di eseguire modifiche sospette di ogni tipo.
Le operazioni di un browser web potrebbero invece stabilire connessioni esterne a server remoti per svariati motivi, in particolare per scaricare ulteriori payloads maligni.
Possiamo aggiungere che non ci sono segni sospetti nell'analisi dinamica sul cercare di 'nascondersi'.

Conclusione: Il file iexplore.exe sembra essere legittimo e non mostra comportamenti sospetti durante l'analisi dinamica. Pertanto, possiamo concludere che non è maligno.