Report Esercizio

W21-D5

Redatto da Andrea Sciattella

20/07/2024

TRACCIA

Un giovane dipendente neoassunto segnala al reparto tecnico la presenza di un programma sospetto.

Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC. Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer (no, non ridete ragazzi)

Come membro senior del SOC ti è richiesto di convincere il dipendente che il file non è maligno.

Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione.

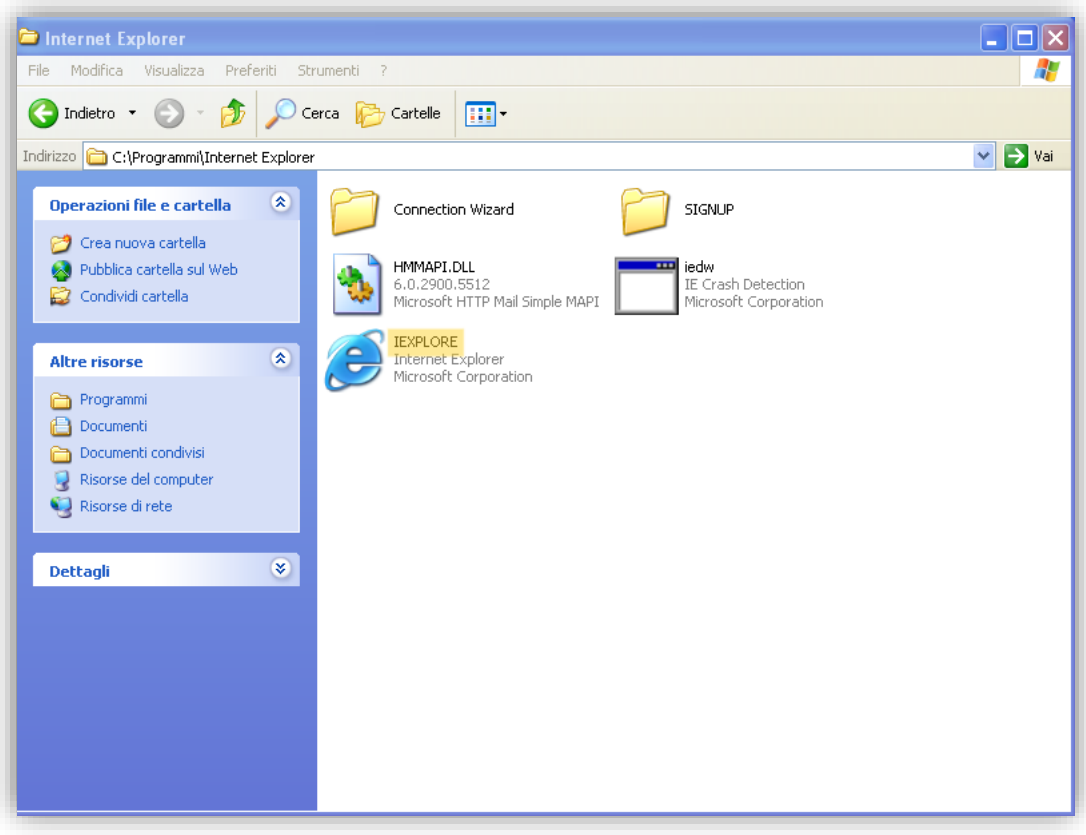
No disassembly no debug o similari VirusTotal non basta, ovviamente Non basta dire iexplorer è Microsoft è buono, punto.

TRACCIA

Per convincere il giovane dipendente che il file IEXPLORE.EXE non è maligno, è importante adottare un approccio metodico utilizzando strumenti di analisi statica e dinamica di base, spiegando ogni passaggio in modo chiaro e dettagliato.

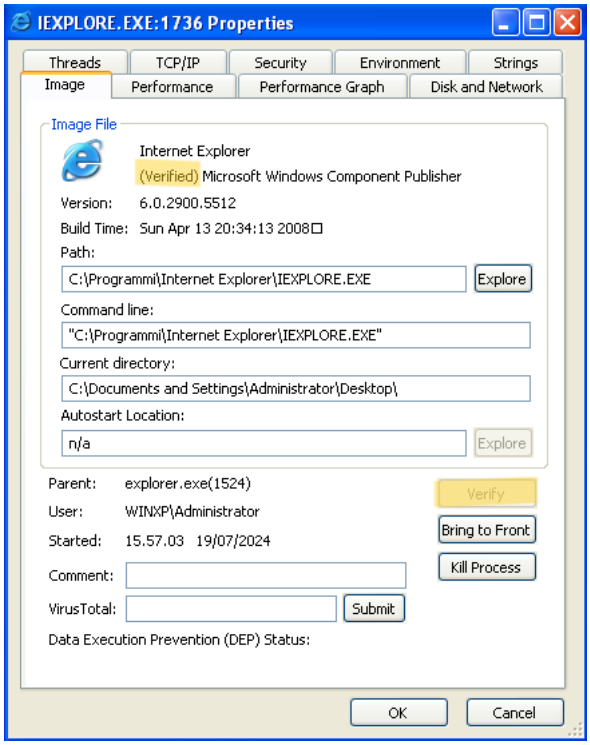
1. Analisi Statica Base

Possiamo mostrare al dipendente che il file si trova in C:\Program Files\Internet Explorer\IEXPLORE.EXE, che è la posizione standard per l'eseguibile di Internet Explorer, mostrando anche l'azienda produttrice.



- Proprietà del file:

Per verificare le proprietà del file, utilizzeremo il tool fornito dalla Suite Sysinternals Process Explorer che alla scheda "Image" conferma la firma da Microsoft Corporation. Una firma valida e affidabile indica che il file è autentico e non alterato.



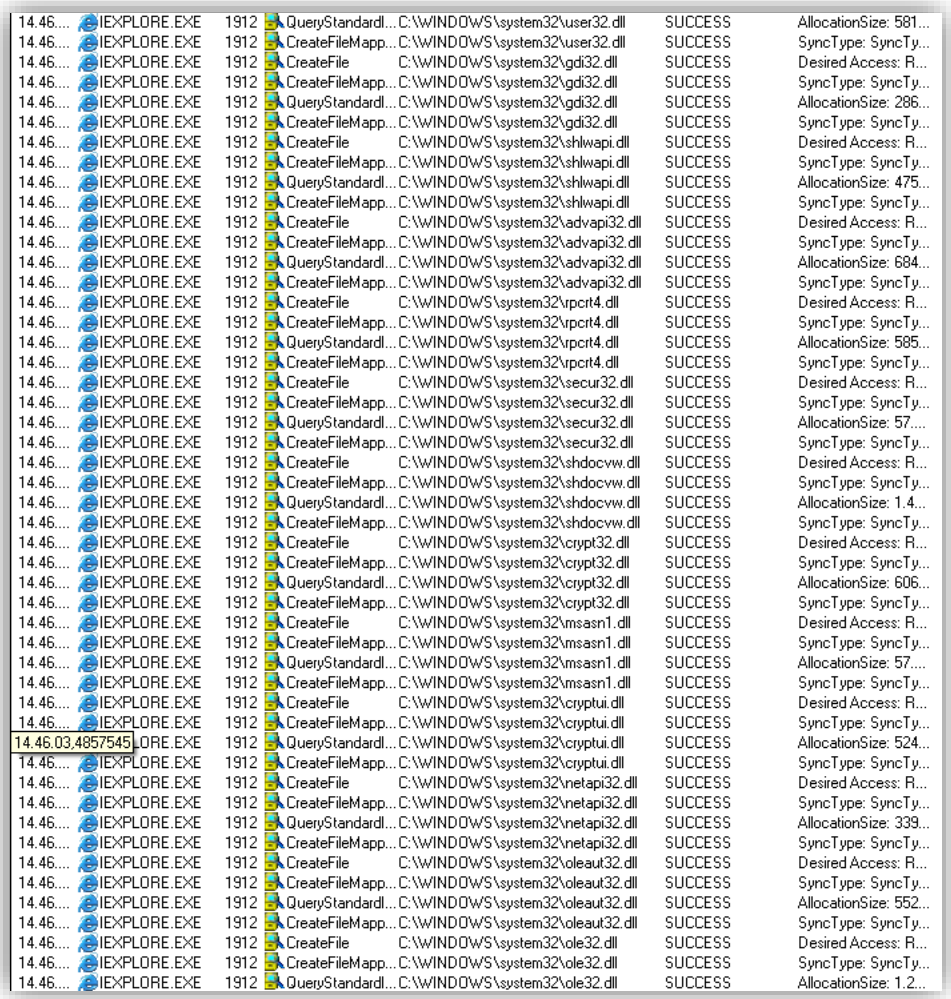
- Per verificare l'autenticità del programma, apriamo la scheda "Image", e selezioniamo il tasto in basso a destra "verify". Se l'applicazione risulta verificata e sicura, nel nome in alto a sinistra apparirà la scritta "Verified" che confermerà l'applicazione.

2. Analisi Dinamica Base

Possiamo eseguire il programma in un ambiente isolato per poter monitorare il comportamento del file usando strumenti della suite “SysInternals” come Process Monitor (ProcMon).

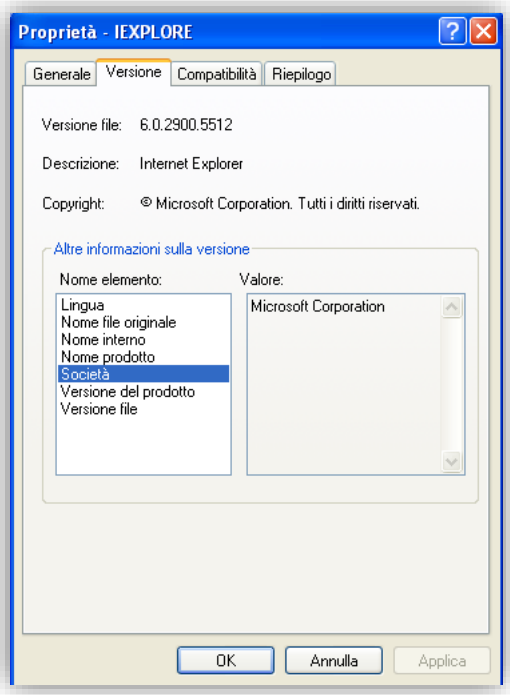
- Monitoraggio dei processi:

Verifichiamo che IEXPLORE.EXE non esegua operazioni sospette come modificare file di sistema critici, connettersi a domini sconosciuti, o scaricare/eseguire altri file eseguibili.



14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\user32.dll	SUCCESS	AllocationSize: 581...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\user32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	AllocationSize: 286...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\gdi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	AllocationSize: 475...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	AllocationSize: 684...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\advapi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	AllocationSize: 585...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\secur32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\secur32.dll	SUCCESS	AllocationSize: 57....
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\secur32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	AllocationSize: 1.4...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\crypt32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\crypt32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\crypt32.dll	SUCCESS	AllocationSize: 606...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\crypt32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\msasn1.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\msasn1.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\msasn1.dll	SUCCESS	AllocationSize: 57....
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\msasn1.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\cryptui.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\cryptui.dll	SUCCESS	SyncType: SyncTy...
14.46.03.4857545	LORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\cryptui.dll	SUCCESS	AllocationSize: 524...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\cryptui.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\netapi32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\netapi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\netapi32.dll	SUCCESS	AllocationSize: 339...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\netapi32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	AllocationSize: 552...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\oleaut32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	CreateFile	C:\WINDOWS\system32\ole32.dll	SUCCESS	Desired Access: R...
14.46....	IEXPLORE.EXE	1912	CreateFileMapp...	C:\WINDOWS\system32\ole32.dll	SUCCESS	SyncType: SyncTy...
14.46....	IEXPLORE.EXE	1912	QueryStandardI...	C:\WINDOWS\system32\ole32.dll	SUCCESS	AllocationSize: 1.2...

- Come possiamo osservare, IEXPLORE.EXE carica DLL (Librerie dinamiche) confermate e completamente affidabile, confermando quindi la sua integrità.



- Come altra conferma abbiamo ogni dettaglio della versione nella scheda “Versione” di ProcMon, che conferma ancora la produzione da parte della casa Microsoft.

CONCLUSIONE

Alla fine di questa analisi, dovrebbe essere chiaro che **IEXPLORE.EXE** è un file legittimo Microsoft Internet Explorer e non rappresenta una minaccia per il sistema.

Presentando i dati raccolti e spiegando il processo, siamo stati in grado di convincere il dipendente della non malignità del file.

A volte però, è possibile che un malware possa utilizzare il nome di un processo legittimo come IEXPLORE.EXE per mascherare le sue azioni. Questa azione è nota come "process hollowing" o "process injection".

Quindi come best practices, è sempre consigliato di svolgere controlli approfonditi con scanner anti-malware e anti-virus per evitare falle nel sistema.