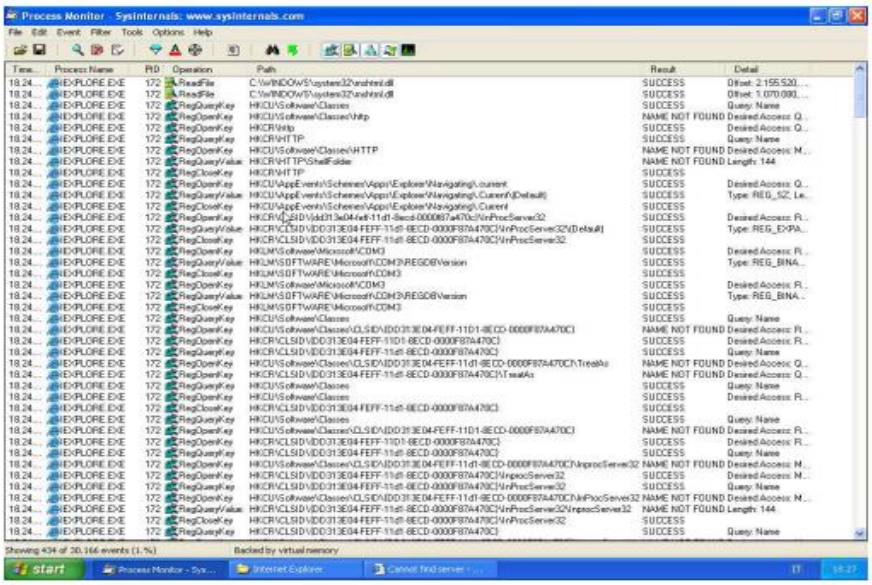
M6 D2

ESERCIZIO

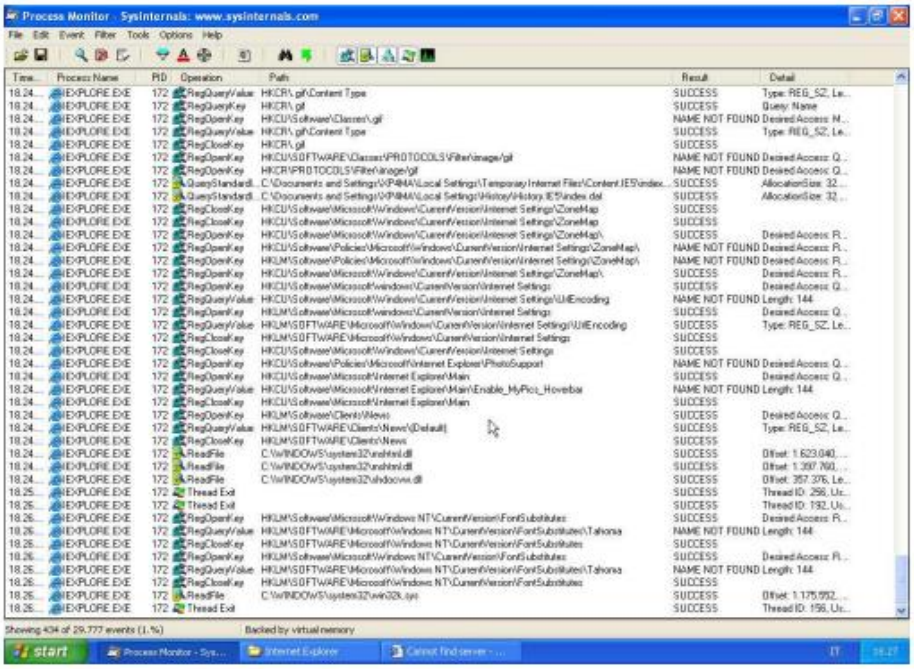
Per analisi del file sospetto IEXPLORE.EXE , si è utilizzato Procmon

Andiamo a eseguire ProcMon, impostiamo un filtro per l'eseguibile "IEXPLORE.EXE", lanciamolo e attendiamo la fine del monitoraggio.



Osservando attentamente l'attività registrata dal programma, notiamo che non vi sono tentativi di connessione non correlati al software in questione ne la creazione o la modifica di file di sistema critici. Si noti anche l'assenza di processi figlio sospetti non riconducibili a Internet Explorer stesso. Anche l'accesso alle sezioni di registro è limitato alle chiavi solitamente in uso dal browser.

Possiamo dunque rassicurare l'impiegato sulla legittimità del software in questione con certezza quasi assoluta.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path Result Detail
18.24... IEXPLORE.EXE 172 RegQueryValue HKCR\.gif\Content Type SUCCESS Type: REG_SZ, Le...
18.24... IEXPLORE.EXE 172 RegQueryKey HKCR\.gif SUCCESS Query: Name
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Classes\.gif NAME NOT FOUND Desired Access: M...
18.24... IEXPLORE.EXE 172 RegQueryValue HKCR\.gif\Content Type SUCCESS Type: REG_SZ, Le...
18.24... IEXPLORE.EXE 172 RegCloseKey HKCR\.gif SUCCESS
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\SOFTWARE\Classes\PROTOCOLS\Filter\image/gif NAME NOT FOUND Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegOpenKey HKCR\PROTOCOLS\Filter\image/gif NAME NOT FOUND Desired Access: Q...
18.24... IEXPLORE.EXE 172 QueryStandardI... C:\Documents and Settings\VIPMMA\Local Settings\Temporary Internet Files\Content.IE5\index... SUCCESS AllocationSize: 32...
18.24... IEXPLORE.EXE 172 QueryStandardI... C:\Documents and Settings\VIPMMA\Local Settings\History\History.IE5\index.dat SUCCESS AllocationSize: 32...
18.24... IEXPLORE.EXE 172 RegCloseKey HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap SUCCESS
18.24... IEXPLORE.EXE 172 RegCloseKey HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap SUCCESS
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ SUCCESS Desired Access: R...
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ NAME NOT FOUND Desired Access: R...
18.24... IEXPLORE.EXE 172 RegOpenKey HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ NAME NOT FOUND Desired Access: R...
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ SUCCESS Desired Access: R...
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings SUCCESS Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegQueryValue HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\UrlEncoding NAME NOT FOUND Length: 144
18.24... IEXPLORE.EXE 172 RegOpenKey HKLM\Software\Microsoft\windows\CurrentVersion\Internet Settings SUCCESS Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\UrlEncoding SUCCESS Type: REG_SZ, Le...
18.24... IEXPLORE.EXE 172 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings SUCCESS
18.24... IEXPLORE.EXE 172 RegCloseKey HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings SUCCESS
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Policies\Microsoft\Internet Explorer\PhotoSupport NAME NOT FOUND Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegOpenKey HKCU\Software\Microsoft\Internet Explorer\Main SUCCESS Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegQueryValue HKCU\Software\Microsoft\Internet Explorer\Main\Enable_MyPics_Hoverbar NAME NOT FOUND Length: 144
18.24... IEXPLORE.EXE 172 RegCloseKey HKCU\Software\Microsoft\Internet Explorer\Main SUCCESS
18.24... IEXPLORE.EXE 172 RegOpenKey HKLM\Software\Clients\News SUCCESS Desired Access: Q...
18.24... IEXPLORE.EXE 172 RegQueryValue HKLM\SOFTWARE\Clients\News\(Default) SUCCESS Type: REG_SZ, Le...
18.24... IEXPLORE.EXE 172 RegCloseKey HKLM\SOFTWARE\Clients\News SUCCESS
18.24... IEXPLORE.EXE 172 ReadFile C:\WINDOWS\system32\urlmon.dll SUCCESS Offset: 1,623,040, ...
18.24... IEXPLORE.EXE 172 ReadFile C:\WINDOWS\system32\urlmon.dll SUCCESS Offset: 1,397,760, ...
18.24... IEXPLORE.EXE 172 ReadFile C:\WINDOWS\system32\shdocvw.dll SUCCESS Offset: 357,376, Le...
18.25... IEXPLORE.EXE 172 Thread Exit SUCCESS Thread ID: 256, Us...
18.25... IEXPLORE.EXE 172 Thread Exit SUCCESS Thread ID: 732, Us...
18.26... IEXPLORE.EXE 172 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes SUCCESS Desired Access: R...
18.26... IEXPLORE.EXE 172 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma NAME NOT FOUND Length: 144
18.26... IEXPLORE.EXE 172 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes SUCCESS
18.26... IEXPLORE.EXE 172 RegOpenKey HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes SUCCESS Desired Access: R...
18.26... IEXPLORE.EXE 172 RegQueryValue HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma NAME NOT FOUND Length: 144
18.26... IEXPLORE.EXE 172 RegCloseKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes SUCCESS
18.26... IEXPLORE.EXE 172 ReadFile C:\WINDOWS\system32\win32k.sys SUCCESS Offset: 1,175,552, ...
18.26... IEXPLORE.EXE 172 Thread Exit SUCCESS Thread ID: 156, Us...
Showing 434 of 29,777 events (1.%) Backed by virtual memory
start
Process Monitor - Sys...
Internet Explorer
Cannot find server - ...
IT
16:27