

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

Process Monitor - Sysinternals: www.sysinternals.com							
File Edit View Filter Tools Options Help							
Time...	Process Name	PID	Operation	Path	Result	Detail	
18.24...	EXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\winhttp.dll	SUCCESS	Offset: 2155,520...	
18.24...	EXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\winhttp.dll	SUCCESS	Offset: 1,070,080...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\http	NAME NOT FOUND	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\http	SUCCESS	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\HTTP	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\HTTP	NAME NOT FOUND	Desired Access: M...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\HTTP	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKCU\Software\Classes\ShellDefault	NAME NOT FOUND	Length: 144	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\HTTP	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\AppData\Local\Schemes\Apps\Explore\Navigating\Current	SUCCESS	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKCU\AppData\Local\Schemes\Apps\Explore\Navigating\Current(Default)	SUCCESS	Type: REG_SZ, Le...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\AppData\Local\Schemes\Apps\Explore\Navigating\Current	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{dd313e4f-11d1-8e0c-0000f8a740c}\InProcServer32	SUCCESS	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32(Default)	SUCCESS	Type: REG_EXPAN...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKLM\Software\Microsoft\COM3	SUCCESS	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKLM\SOFTWARE\Microsoft\COM3\REGDBVersion	SUCCESS	Type: REG_BINARY	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKLM\SOFTWARE\Microsoft\COM3	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKLM\Software\Microsoft\COM3	SUCCESS	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKLM\SOFTWARE\Microsoft\COM3\REGDBVersion	SUCCESS	Type: REG_BINARY	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKLM\SOFTWARE\Microsoft\COM3	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	NAME NOT FOUND	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\TreatAs	NAME NOT FOUND	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\TreatAs	NAME NOT FOUND	Desired Access: Q...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes	SUCCESS	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	NAME NOT FOUND	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS	Desired Access: R...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	NAME NOT FOUND	Desired Access: M...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	SUCCESS	Desired Access: M...	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	SUCCESS	Query: Name	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	NAME NOT FOUND	Desired Access: M...	
18.24...	EXPLORE.EXE	172	RegOpenValue	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32\InProcServer32	NAME NOT FOUND	Length: 144	
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}\InProcServer32	SUCCESS		
18.24...	EXPLORE.EXE	172	RegOpenKey	HKCR\CLSID\{DD313E4F-11D1-8E0C-0000F8A740C}	SUCCESS	Query: Name	

Osservando attentamente l'attività registrata dal programma, notiamo che non vi sono tentativi di connessione non correlati al software in questione né 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 assicurare 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						
<div> </div>						
Time...	Process Name	PID	Operation	Path	Result	Detail
18.24...	ieXPLORE.EXE	172	RegQueryValue	HKCR,gli\Content Type	SUCCESS	Type: REG_SZ, Le...
18.24...	ieXPLORE.EXE	172	RegQueryKey	HKCR,gli	SUCCESS	Query: Name
18.24...	ieXPLORE.EXE	172	RegOpenKey	HKCU\Software\Classes\gli	NAME NOT FOUND	Desired Access: M...
18.24...	ieXPLORE.EXE	172	RegQueryValue	HKCR,gli\Content Type	SUCCESS	Type: REG_SZ, Le...
18.24...	ieXPLORE.EXE	172	RegQueryKey	HKCR,gli	SUCCESS	
18.24...	ieXPLORE.EXE	172	RegOpenKey	HKCU\SOFTWARE\Classes\PROTOCOLS\Filer\image\gli	NAME NOT FOUND	Desired Access: Q...
18.24...	ieXPLORE.EXE	172	RegOpenKey	HKCR\PROTOCOLS\Filer\image\gli	NAME NOT FOUND	Desired Access: Q...
18.24...	ieXPLORE.EXE	172	QueryStandard...	C:\Documents and Settings\VP4MA\Local Settings\Temporary Internet Files\Content.IE5\index...	SUCCESS	AllocationSize: 32...
18.24...	ieXPLORE.EXE	172	QueryStandard...	C:\Documents and Settings\VP4MA\Local Settings\History\History.IE5\index.d...	SUCCESS	AllocationSize: 32...
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	
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\UIEncoding	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	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\UIEncoding	SUCCESS	Type: REG_SZ, Le...
18.24...	ieXPLORE.EXE	172	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings	SUCCESS	
18.24...	ieXPLORE.EXE	172	RegOpenKey	HKCU\Software\Policies\Microsoft\Internet Explorer\PhishingSupport	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_MyPic...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\Classes\News	SUCCESS	Desired Access: Q...
18.24...	ieXPLORE.EXE	172	RegQueryValue	HKLM\SOFTWARE\Classes\News\{Default}	SUCCESS	Type: REG_SZ, Le...
18.24...	ieXPLORE.EXE	172	RegQueryValue	HKLM\SOFTWARE\Classes\News	SUCCESS	
18.24...	ieXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\mhtml.dll	SUCCESS	Offset: 1,623,040, ...
18.24...	ieXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\mhtml.dll	SUCCESS	Offset: 1,397,760, ...
18.24...	ieXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\shdocvw.dll	SUCCESS	Offset: 357,376, U...
18.25...	ieXPLORE.EXE	172	Thread Exit		SUCCESS	Thread ID: 256, U...
18.25...	ieXPLORE.EXE	172	Thread Exit		SUCCESS	Thread ID: 192, U...
18.25...	ieXPLORE.EXE	172	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	Desired Access: R...
18.25...	ieXPLORE.EXE	172	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma	NAME NOT FOUND	Length: 144
18.25...	ieXPLORE.EXE	172	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	
18.25...	ieXPLORE.EXE	172	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	Desired Access: R...
18.25...	ieXPLORE.EXE	172	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma	NAME NOT FOUND	Length: 144
18.25...	ieXPLORE.EXE	172	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes	SUCCESS	
18.25...	ieXPLORE.EXE	172	ReadFile	C:\WINDOWS\system32\win32k.sys	SUCCESS	Offset: 1,175,852, ...
18.25...	ieXPLORE.EXE	172	Thread Exit		SUCCESS	Thread ID: 156, U...
Showing 434 of 29,777 events (1.%)						
Backed by virtual memory						
<div><div>start</div><div><div>Process Monitor - Sys...</div><div>Internet Explorer</div><div>Cannot find server ...</div><div>IT</div><div>18.25...</div></div></div>						