TRACCIA:
Un giovane dipendente neo assunto 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:\Programmi\Internet Explorer.

ANALISI STATICA

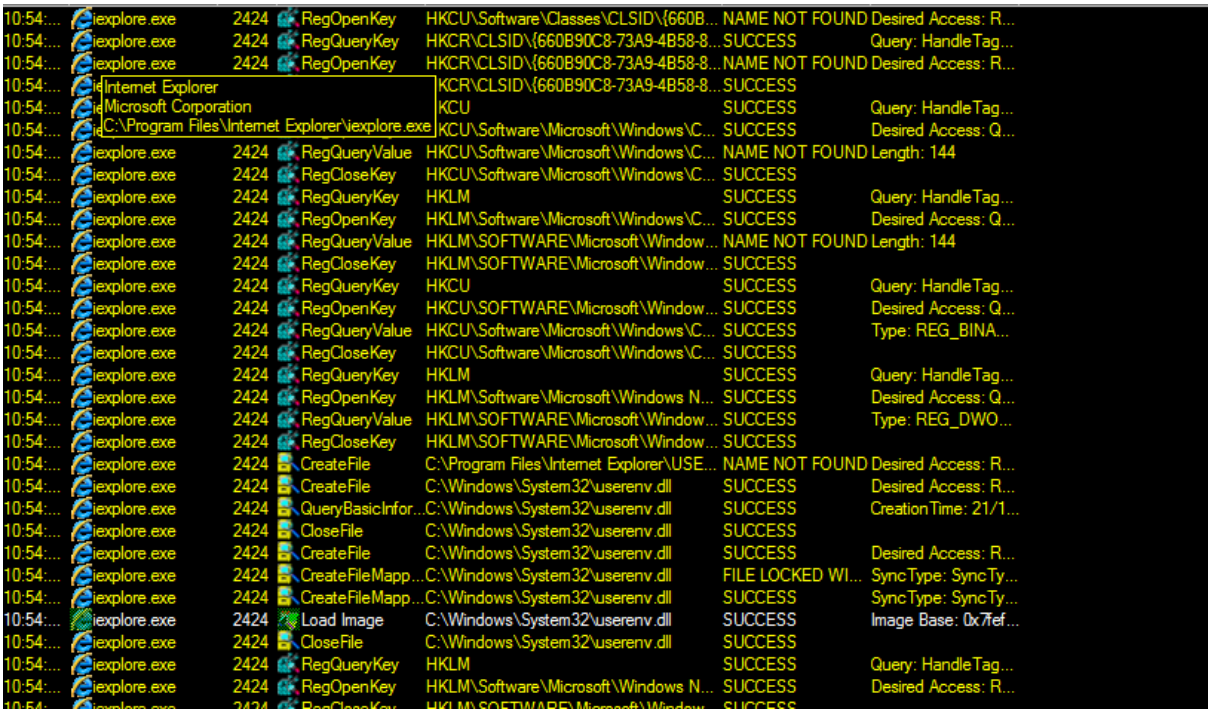
Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT
0000DE34	N/A	0000DE0C	0000DE10	0000DE14	0000DE18	0000DE
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFFFF	FFFFFFFF	0000F6A8	0000900
KERNEL32.dll	56	0000F728	FFFFFFFF	FFFFFFFF	0000F698	0000907
USER32.dll	9	0000F8F0	FFFFFFFF	FFFFFFFF	0000F68C	0000923
msvcrt.dll	29	0000F940	FFFFFFFF	FFFFFFFF	0000F680	0000928
ntdll.dll	3	0000FA30	FFFFFFFF	FFFFFFFF	0000F674	0000937
SHLWAPI.dll	23	0000FA50	FFFFFFFF	FFFFFFFF	0000F668	0000939
SHELL32.dll	7	0000FB10	FFFFFFFF	FFFFFFFF	0000F65C	0000945
ole32.dll	5	0000FB50	FFFFFFFF	FFFFFFFF	0000F650	0000949
iertutil.dll	14	0000FB80	FFFFFFFF	FFFFFFFF	0000F640	000094C
urlmon.dll	3	0000FBF8	FFFFFFFF	FFFFFFFF	0000F634	0000954

advapi32.dll: Contiene le funzioni di API avanzate per la manipolazione di processi, utenti e autorizzazioni di sicurezza nel sistema operativo Windows.
kernel32.dll: È una delle librerie principali del kernel di Windows
user32.dll: Contiene le funzioni per la gestione dell'interfaccia utente di Windows
msvcrt.dll: Questa libreria fornisce le implementazioni delle funzioni standard del linguaggio C (C runtime library) utilizzate dai programmi C e C++ compilati con il compilatore di Microsoft Visual C++.
rtdll.dll: Non è una libreria di sistema standard
shlwapi.dll: Fornisce funzioni di supporto per la shell di Windows
shell32.dll: Contiene le funzioni e le risorse utilizzate per implementare la shell di Windows, inclusi elementi del desktop, finestre di esplorazione dei file e menu di contesto.
ole32.dll: È una libreria che fornisce le funzionalità per implementare e utilizzare i servizi COM (Component Object Model)

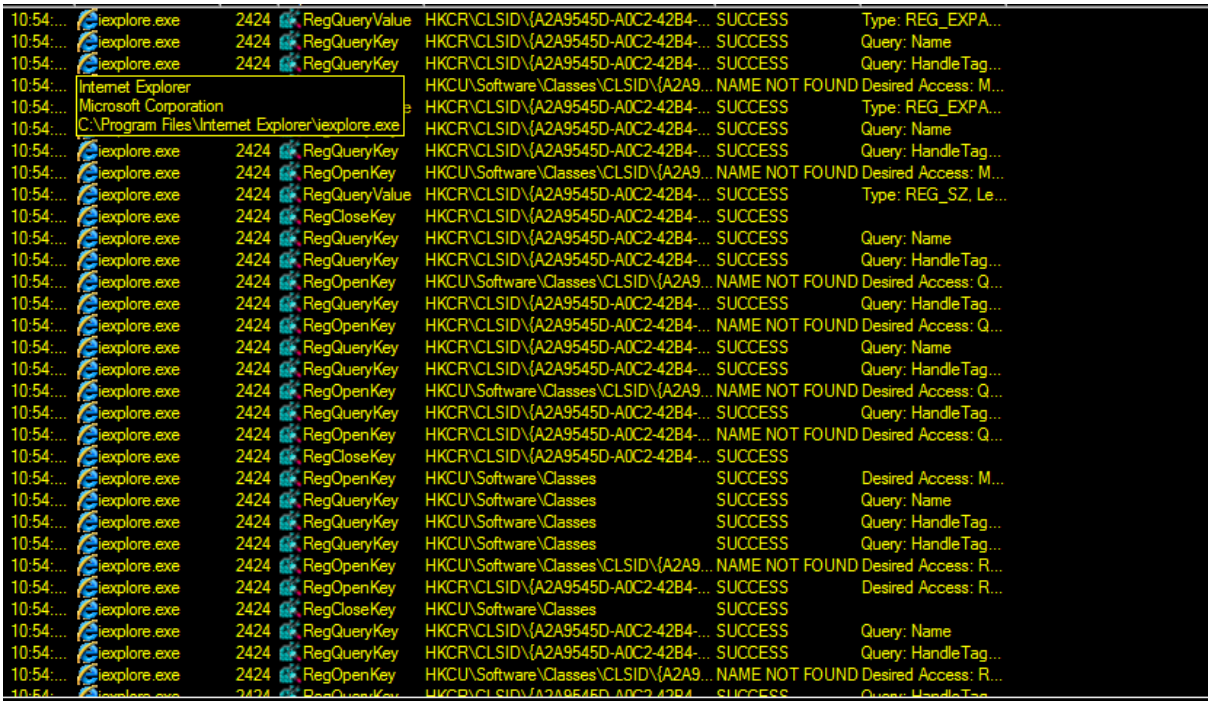
iertutl.dll: Solitamente non è una libreria di sistema standard di Windows. Potrebbe essere specifica per Internet Explorer o per componenti correlati.
urlmon.dll: Contiene funzioni per la gestione di URL e protocolli Internet, inclusi il download di file, la navigazione web e le richieste HTTP.

ANALISI DINAMICA

10:54:...	svchost.exe	1456	UDP Receive	ff02::c:ssdp -> user-PC:49450	SUCCESS	Length: 146, seqn...
10:54:...	iexplore.exe	1908	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	1908	RegOpenKey	HKLM\Software\Policies\Microsoft\Inte...	NAME NOT FOUND	Desired Access: Q...
10:54:...	iexplore.exe	1908	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	1908	RegOpenKey	HKCU\Software\Policies\Microsoft\Inte...	NAME NOT FOUND	Desired Access: Q...
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Rpc\Securit...	SUCCESS	Desired Access: R...
10:54:...	iexplore.exe	2424	RegQueryValue	HKLM\SOFTWARE\Microsoft\Rpc\Se...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegCloseKey	HKLM\SOFTWARE\Microsoft\Rpc\Se...	SUCCESS	
10:54:...	iexplore.exe	1908	Thread Create		SUCCESS	Thread ID: 3792
10:54:...	iexplore.exe	2424	RegQueryValue	HKCU\Software\Microsoft\Internet Expl...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegQueryValue	HKLM\SOFTWARE\Microsoft\Internet ...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegQueryKey	HKCU\Software\Microsoft\Internet Expl...	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKCU\Software\Microsoft\Internet Expl...	NAME NOT FOUND	Desired Access: R...
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	NAME NOT FOUND	Desired Access: R...
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Rpc\Securit...	SUCCESS	Desired Access: R...
10:54:...	iexplore.exe	2424	RegQueryValue	HKLM\SOFTWARE\Microsoft\Rpc\Se...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegCloseKey	HKLM\SOFTWARE\Microsoft\Rpc\Se...	SUCCESS	
10:54:...	iexplore.exe	1908	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	1908	RegOpenKey	HKLM\Software\Microsoft\Internet Expl...	SUCCESS	Desired Access: Q...
10:54:...	iexplore.exe	1908	RegQueryKey	HKLM\SOFTWARE\Microsoft\Internet ...	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	1908	RegOpenKey	HKLM\SOFTWARE\Microsoft\Internet ...	NAME NOT FOUND	Desired Access: Q...
10:54:...	iexplore.exe	1908	RegCloseKey	HKLM\SOFTWARE\Microsoft\Internet ...	SUCCESS	
10:54:...	iexplore.exe	1908	ReadFile	C:\Windows\System32\mshtml.dll	SUCCESS	Offset: 6,260,224, ...
10:54:...	iexplore.exe	1908	ReadFile	C:\Windows\System32\mshtml.dll	SUCCESS	Offset: 6,252,032, ...
10:54:...	iexplore.exe	1908	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
10:54:...	iexplore.exe	1908	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
10:54:...	iexplore.exe	1908	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	1908	RegOpenKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...

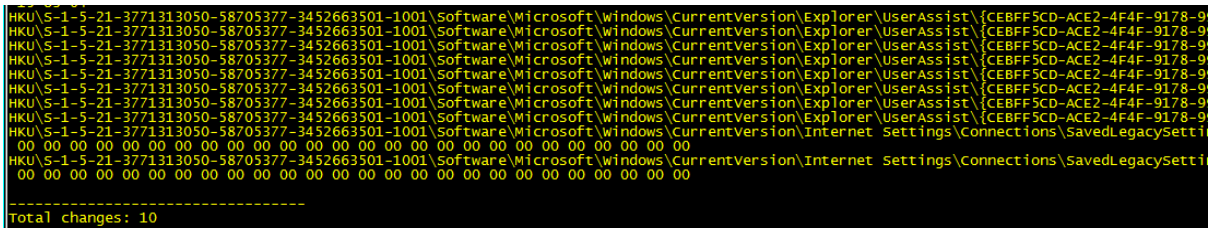


10:54:...	iexplore.exe	2424	RegOpenKey	HKCU\Software\Classes\CLSID\{660B...	NAME NOT FOUND	Desired Access: R...
10:54:...	iexplore.exe	2424	RegQueryKey	HKCR\CLSID\{660B90C8-73A9-4B58-8...	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKCR\CLSID\{660B90C8-73A9-4B58-8...	NAME NOT FOUND	Desired Access: R...
10:54:...	Internet Explorer			KCR\CLSID\{660B90C8-73A9-4B58-8...	SUCCESS	
10:54:...	Microsoft Corporation			KCU	SUCCESS	Query: HandleTag...
10:54:...	C:\Program Files\Internet Explorer\iexplore.exe			KCU\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
10:54:...	iexplore.exe	2424	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: Q...
10:54:...	iexplore.exe	2424	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 144
10:54:...	iexplore.exe	2424	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
10:54:...	iexplore.exe	2424	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKCU\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: Q...
10:54:...	iexplore.exe	2424	RegQueryValue	HKCU\Software\Microsoft\Windows\C...	SUCCESS	Type: REG_BINA...
10:54:...	iexplore.exe	2424	RegCloseKey	HKCU\Software\Microsoft\Windows\C...	SUCCESS	
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
10:54:...	iexplore.exe	2424	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWO...
10:54:...	iexplore.exe	2424	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
10:54:...	iexplore.exe	2424	CreateFile	C:\Program Files\Internet Explorer\USE...	NAME NOT FOUND	Desired Access: R...
10:54:...	iexplore.exe	2424	CreateFile	C:\Windows\System32\userenv.dll	SUCCESS	Desired Access: R...
10:54:...	iexplore.exe	2424	QueryBasicInfor...	C:\Windows\System32\userenv.dll	SUCCESS	CreationTime: 21/1...
10:54:...	iexplore.exe	2424	CloseFile	C:\Windows\System32\userenv.dll	SUCCESS	
10:54:...	iexplore.exe	2424	CreateFile	C:\Windows\System32\userenv.dll	SUCCESS	Desired Access: R...
10:54:...	iexplore.exe	2424	CreateFileMapp...	C:\Windows\System32\userenv.dll	FILE LOCKED WI...	SyncType: SyncTy...
10:54:...	iexplore.exe	2424	CreateFileMapp...	C:\Windows\System32\userenv.dll	SUCCESS	SyncType: SyncTy...
10:54:...	iexplore.exe	2424	Load Image	C:\Windows\System32\userenv.dll	SUCCESS	Image Base: 0x7fef...
10:54:...	iexplore.exe	2424	CloseFile	C:\Windows\System32\userenv.dll	SUCCESS	
10:54:...	iexplore.exe	2424	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
10:54:...	iexplore.exe	2424	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: R...



Possiamo notare attraverso il tool **PROCESS MONITOR** che non ci sono attività sospette,ovvero il programma non va a modificare librerie,non va a fare un escalation di privilegi,inoltre non va a posizionarsi in nessuna cartella anomala,si tratta semplicemente di un programma windows.

Non va nemmeno a creare directory dove posizionare informazioni sensibili catturate.



CONTROLLO CON VIRUSTOTAL

Infatti **virustotal** non identifica nessun tipo di malware all'interno del programma.