



W21D5

MALWARE ANALYSIS

La 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:\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

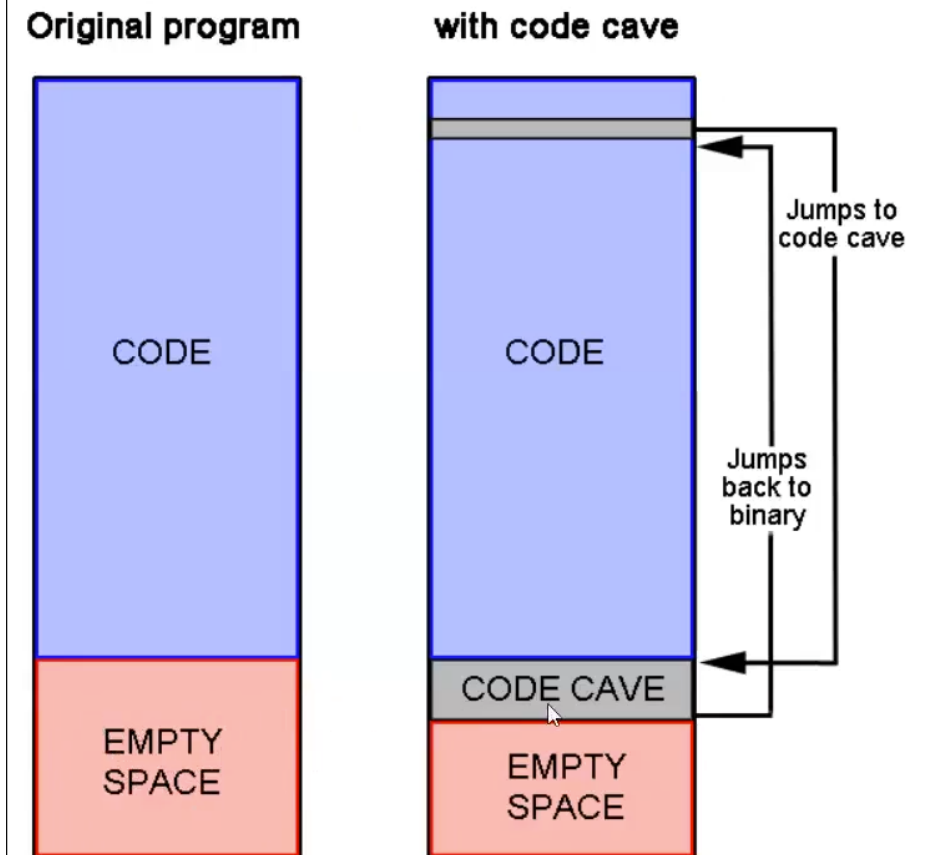
VirusTotal non basta, ovviamente

Non basta dire iexplorer è Microsoft è buono, punto.

Premesse

Il fatto che il file si chiami iexplore.exe non esclude che possa essere un malware, potrebbe creare una copia di un programma normale ed inserire il proprio codice malevolo all'interno (code injection).

Infatti solitamente si disassembla il programma 'regolare' per vedere se ci sono code cave, i malware grazie a questi possono utilizzare istruzioni di jump per 'saltare' a un codice malevolo, potrebbe poi esserci un altro jump che riporta a inizio codice del programma per farlo funzionare normalmente e quindi avere sia l'effetto del codice malevolo avviato che il programma che funziona normalmente.



Controllo certificato e hash

Cliccando sulle proprietà del file possiamo vedere il certificato e l'hash del file.

The screenshot shows the Windows XP desktop with the 'Proprietà - iexplore' window open. The 'Avanzate' tab is selected, showing the 'Dettagli firma:' section. The 'Generale' tab is also visible, showing the 'Sicurezza' section with 'Blanco firme' and 'Nome firmatario: Microsoft Corporation' and 'Algoritmo: sha1'. The 'Certificato' window is open, showing the 'Dettagli' tab with a table of certificate fields.

Campo	Valore
Versione	V2
Autorità emittente	Microsoft Code Signing PCA, Microsoft C.
Numero di serie	61 08 77 5f 00 00 00 00 4a
Algoritmo con classificazi...	sha1
Algoritmo di crittografia c...	RSA
Attributi autenticati	
Tipo contenuto	06 0a 2b 06 01 04 01 82 37 02 01 04
1.3.6.1.4.1.311.2.1.11	30 0c 06 0a 2b 06 01 04 01 82 37 02 01
Digest del messaggio	04 14 1b 4d 68 9e 05 1d fe d3 6c ce 20
1.3.6.1.4.1.311.2.1.12	30 42 a0 24 80 22 00 4d 00 69 00 63 00

The 'Certificato' window also shows the 'Generale' tab with the following information:

- Mostra: <Tutti>
- Versione: V3
- Numero di serie: 61 08 77 5f 00 00 00 00 4a
- Algoritmo della firma elettro...: sha1RSA
- Algoritmo hash della firma: sha1
- Autorità emittente: Microsoft Code Signing PCA, M...
- Valido da: martedì 20 luglio 2010 00:53:10
- Valido fino a: giovedì 20 ottobre 2011 00:53:10
- Sonetto: Microsoft Corporation. M...

Analisi statica con CFF Explorer

Da Virus Total possiamo fare un check del file, da qui risulta essere del 2010, è un file di Microsoft, prendiamo lo Sha1 e vediamo che c'è la firma di Microsoft dovrebbe essere affidabile ma non è detto in quanto potrebbe essere stato attaccato il sistema di Microsoft.

Signers

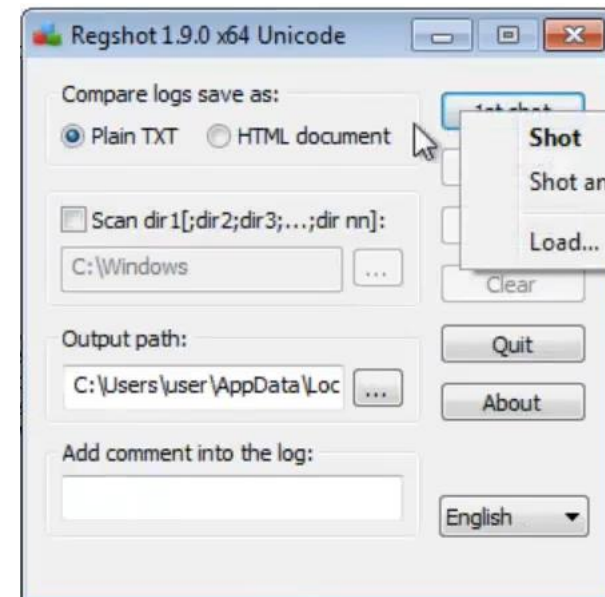
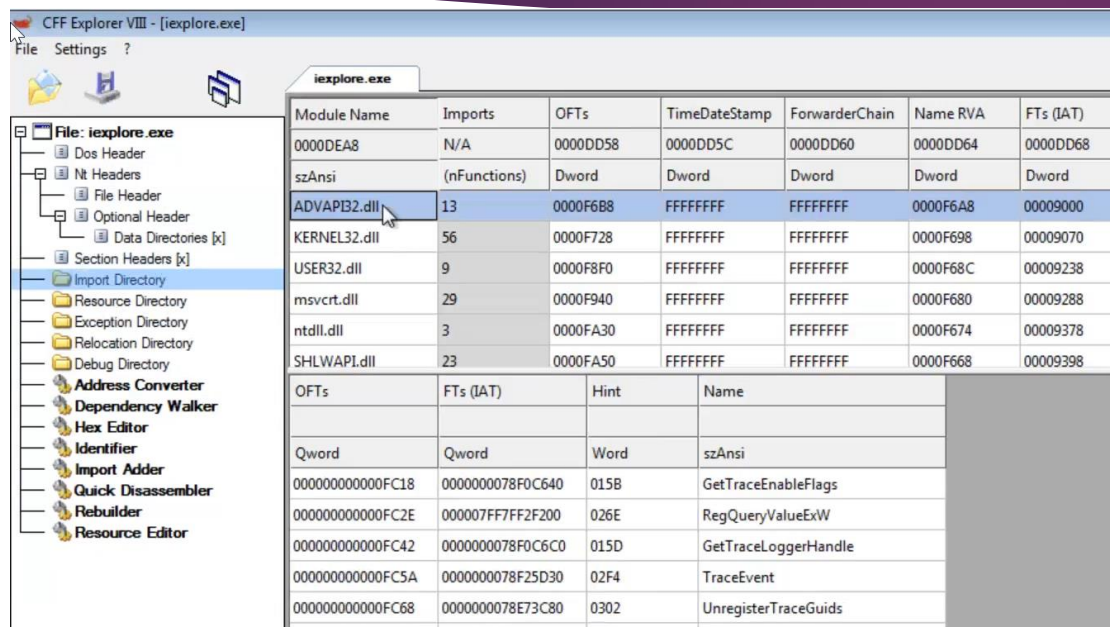
- + Microsoft Corporation
- + Microsoft Code Signing PCA
- + Microsoft Root Certificate Authority

The screenshot shows the CFF Explorer VIII interface with the file 'iexplore.exe' loaded. The left pane displays a tree view of the file's internal structure, including headers, sections, and various directories. The right pane shows two tables of properties.

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

Analisi statica: controllo librerie importate e utilizzo di Regshot

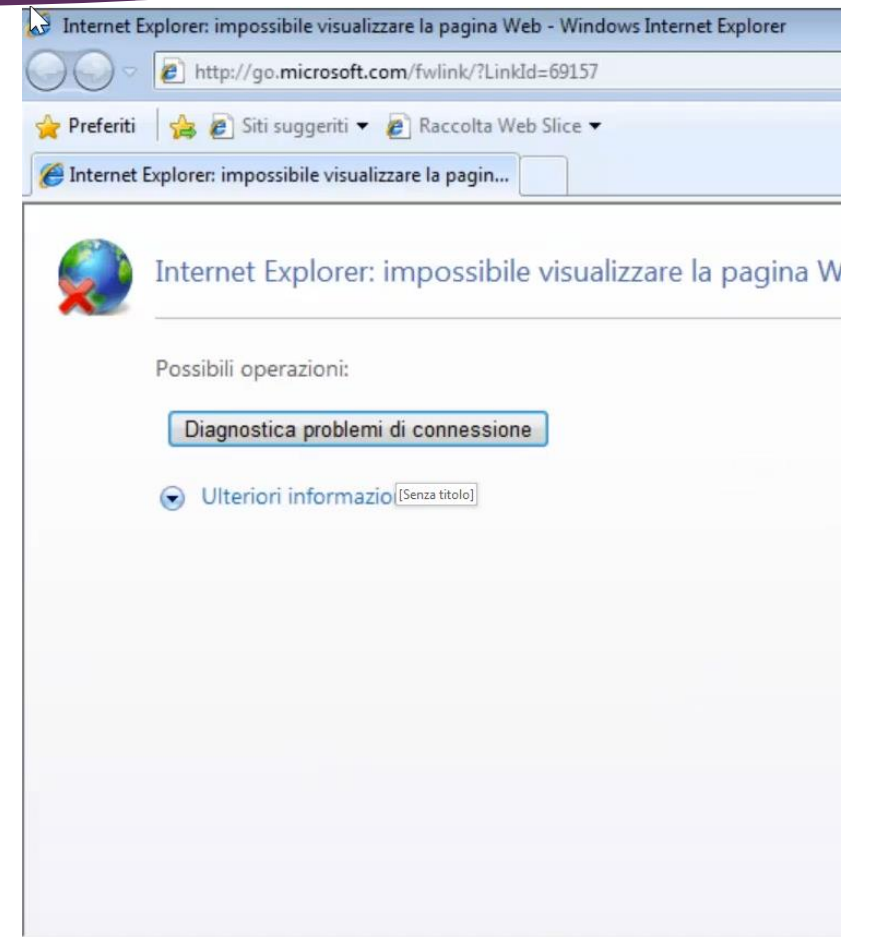
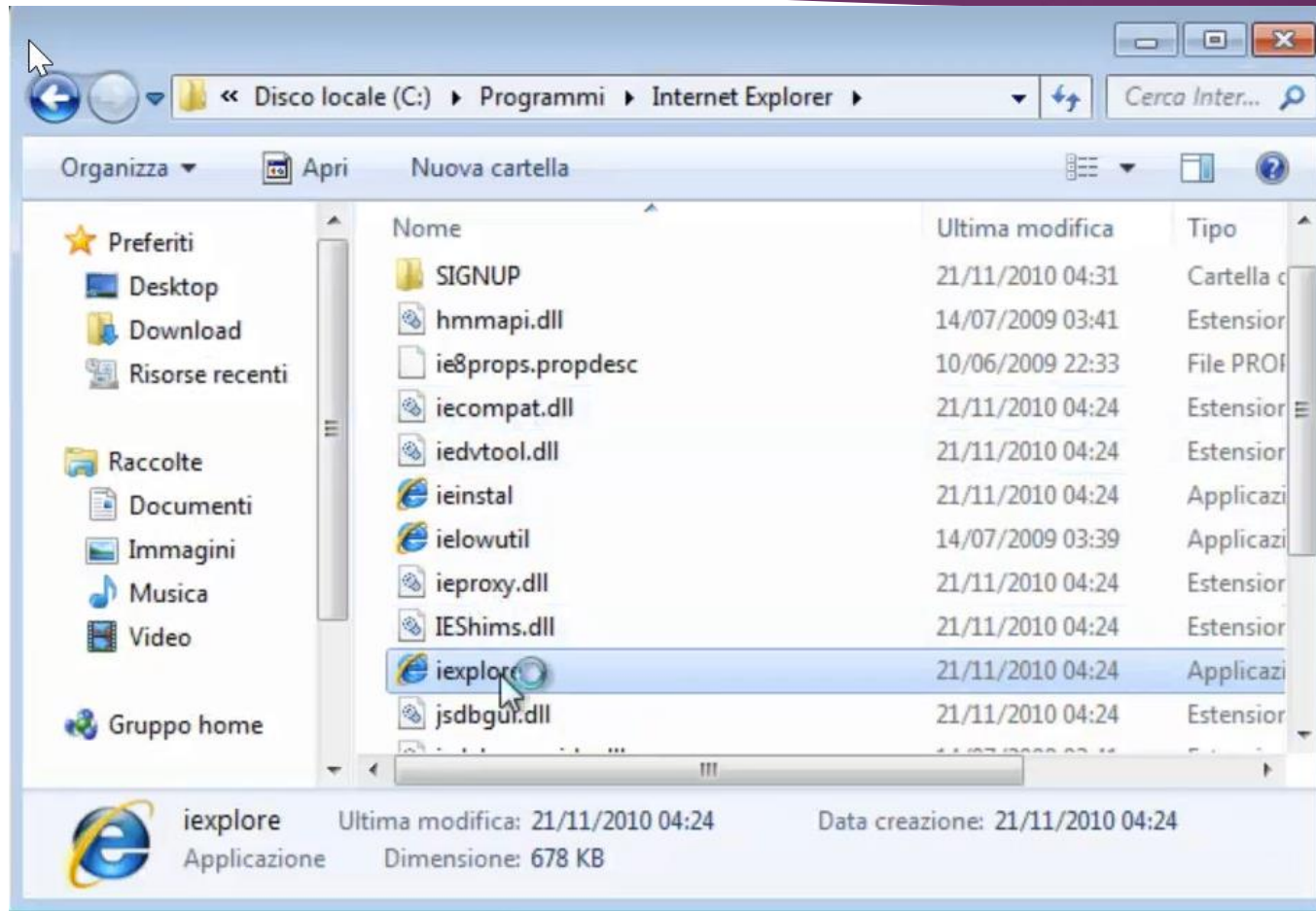


Imports

- + ADVAPI32.dll
- + KERNEL32.dll
- + USER32.dll
- + msvcrt.dll
- + ntdll.dll
- + SHLWAPI.dll
- + SHELL32.dll
- + ole32.dll
- + iertutil.dll
- + urlmon.dll

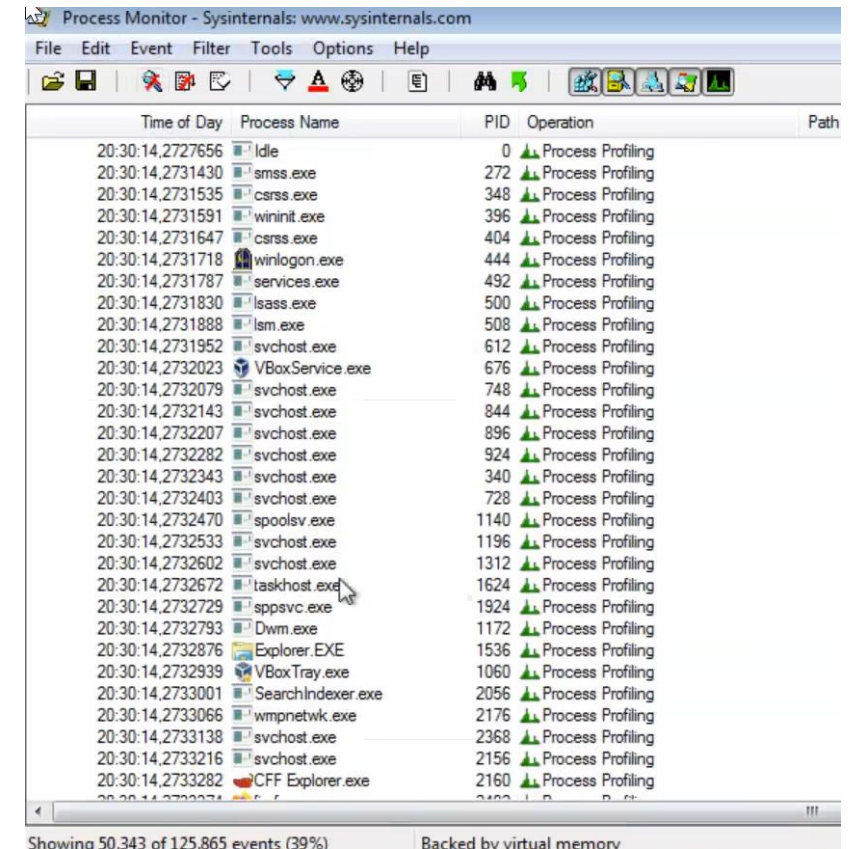
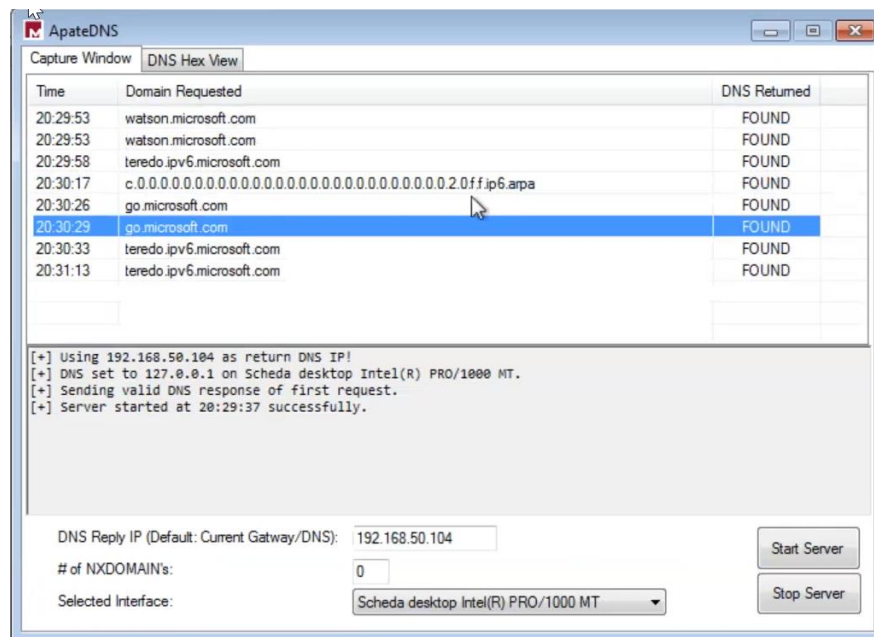
Sempre su CffExplorer possiamo verificare le librerie importate dal file in questione e vedere se sono legittime su Virus Total.
Possiamo verificare i registri con Regshot, prima e dopo avvio file. Avviamo Procmon, Proexec e Apat Dns (da configurare).

Avvio del file



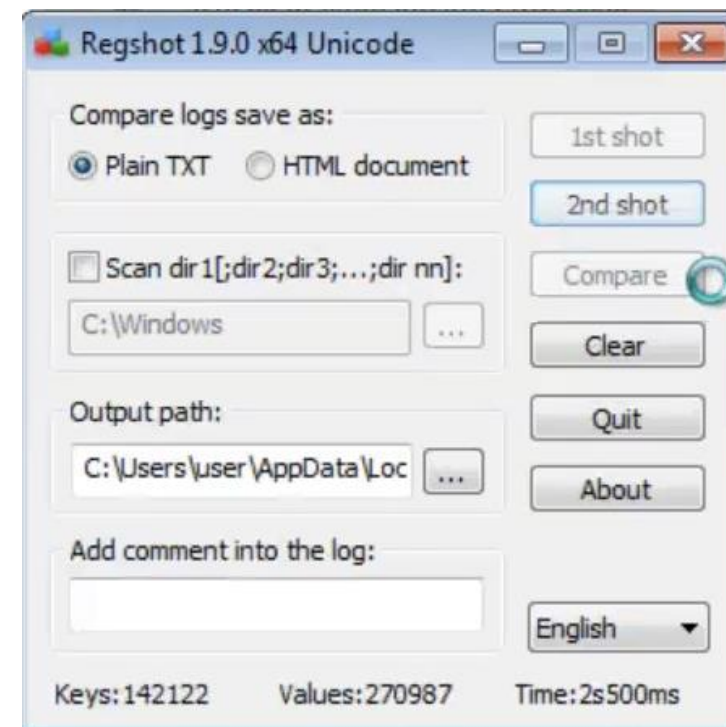
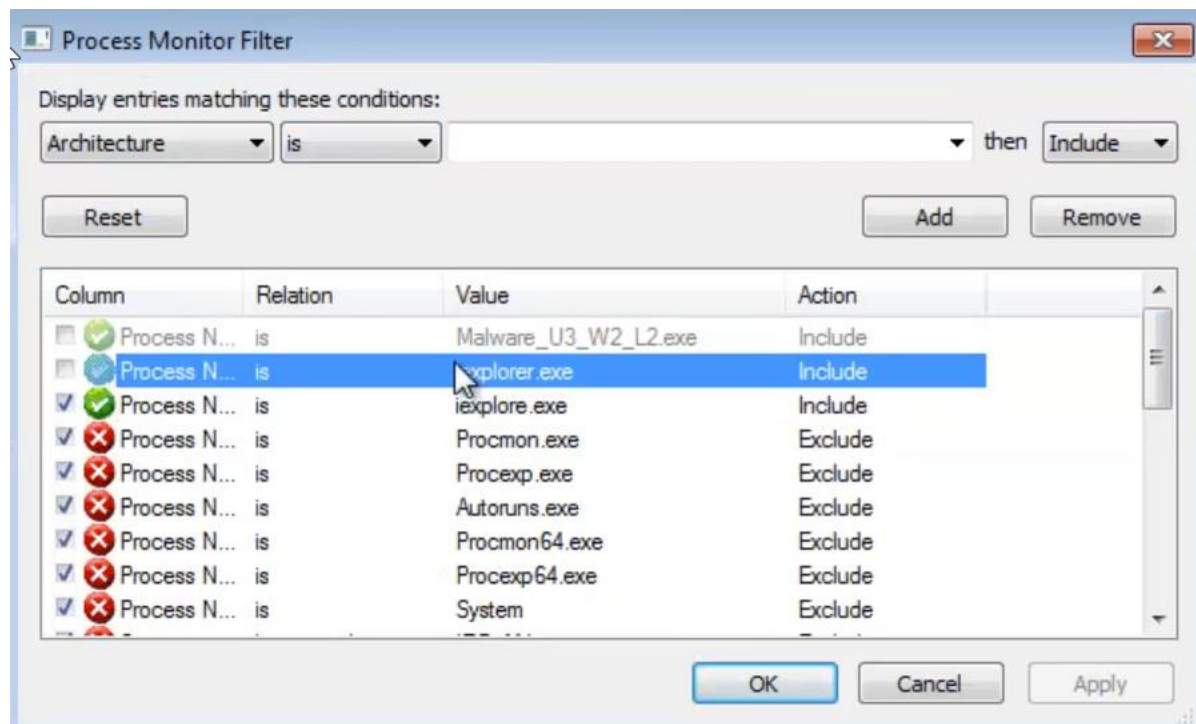
Analisi dinamica: utilizzo Procmon

Con ProcMon possiamo visualizzare le operazioni su file system, processi, threads e attività di rete.



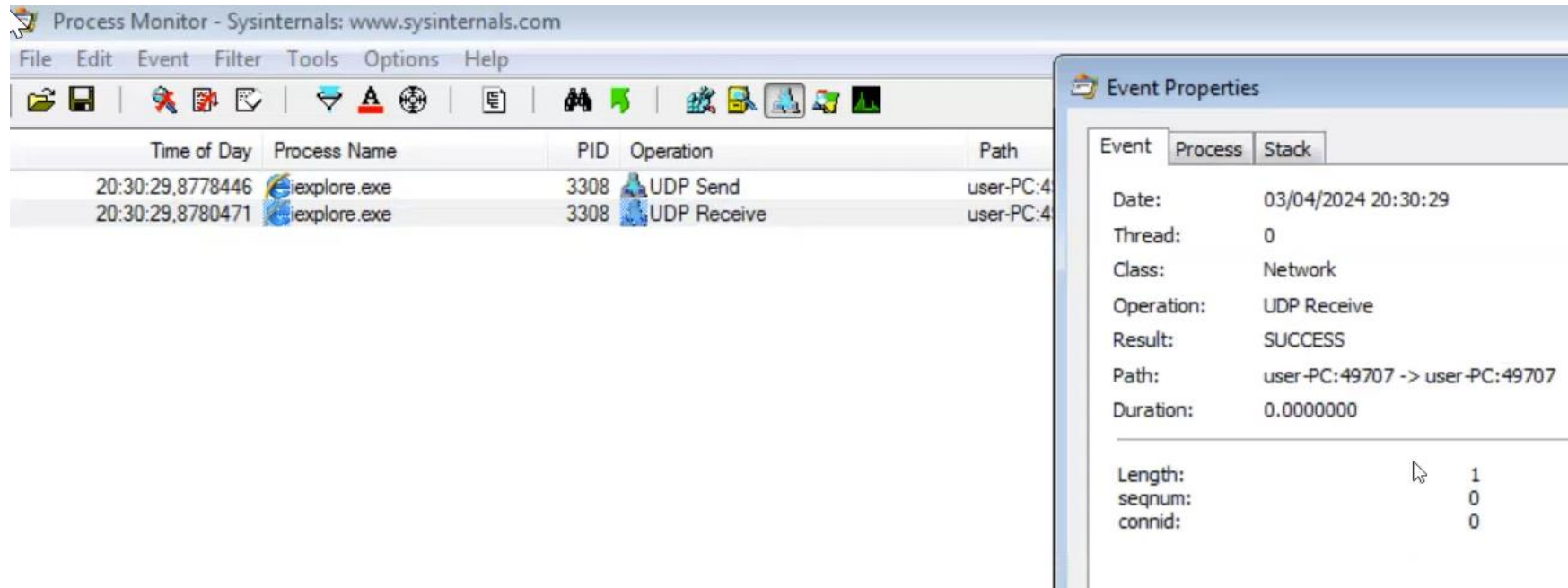
Analisi dinamica: Procmon

Filtro su processo iexplore.exe ed effettuo secondo shot su Regshot e si fa il compare.



Analisi dinamica: Procmon, comunicazione di rete

Questi sotto sono gli unici eventi di rete rilevati, nulla di sospetto.



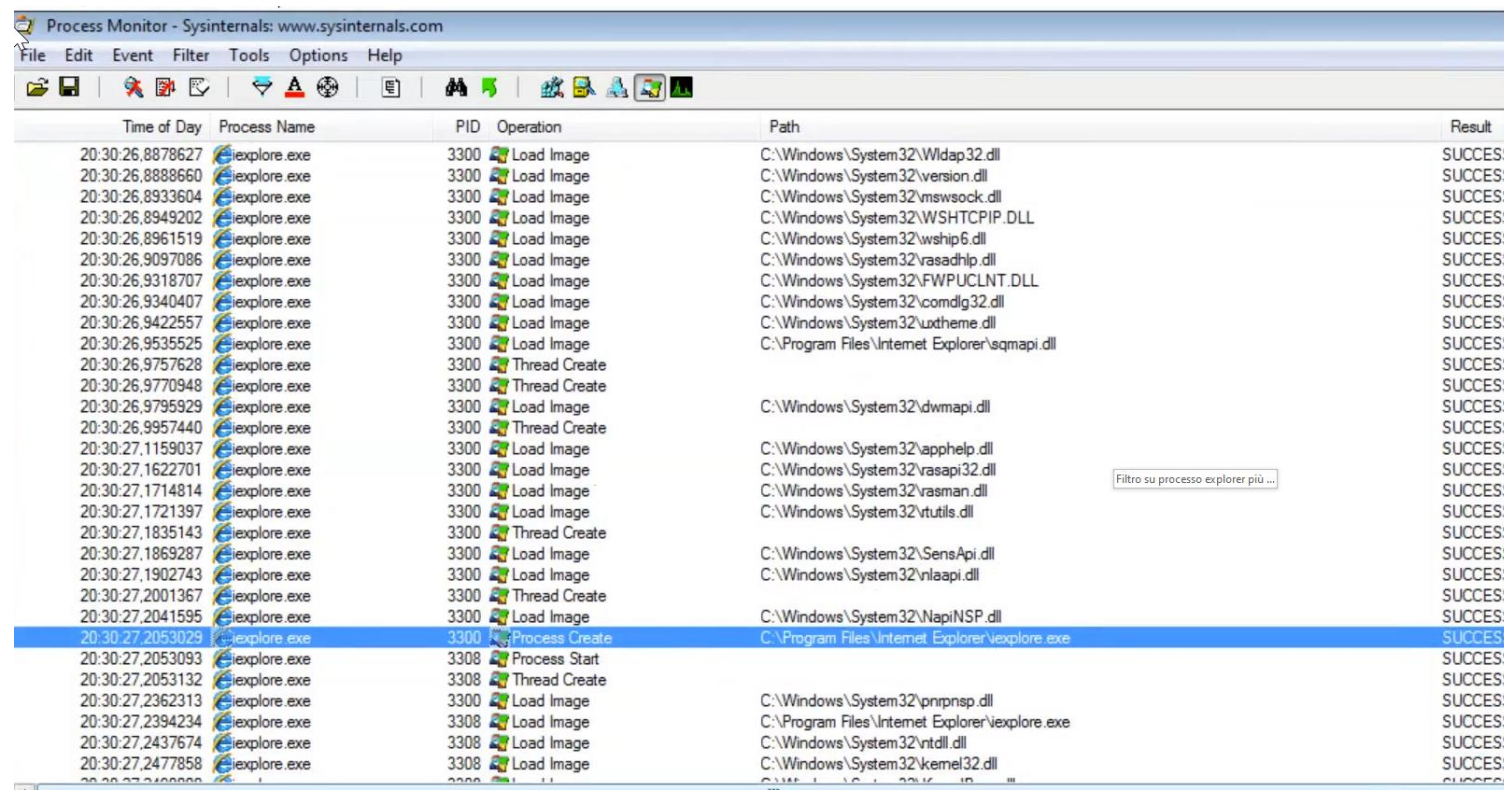
The screenshot displays the Process Monitor (Procmon) application window. The main pane shows a list of events with columns for Time of Day, Process Name, PID, Operation, and Path. Two events are visible, both involving explorer.exe at PID 3308: a UDP Send at 20:30:29,8778446 and a UDP Receive at 20:30:29,8780471. An 'Event Properties' dialog box is open on the right, showing details for the selected 'UDP Receive' event. The dialog includes tabs for Event, Process, and Stack, with the Event tab currently active. The event details show a successful UDP receive operation on the local machine (user-PC:49707) with a duration of 0.0000000.

Time of Day	Process Name	PID	Operation	Path
20:30:29,8778446	explorer.exe	3308	UDP Send	user-PC:4
20:30:29,8780471	explorer.exe	3308	UDP Receive	user-PC:4

Event Properties	
Event	Process
Date:	03/04/2024 20:30:29
Thread:	0
Class:	Network
Operation:	UDP Receive
Result:	SUCCESS
Path:	user-PC:49707 -> user-PC:49707
Duration:	0.0000000
Length:	1
seqnum:	0
connid:	0

Analisi dinamica: Procmon

Vediamo se crea altri processi e se si nasconde e verifico seguendo il pid se termina sempre con lo stesso.



Time of Day	Process Name	PID	Operation	Path	Result
20:30:26,8878627	explorer.exe	3300	Load Image	C:\Windows\System32\Widap32.dll	SUCCESS
20:30:26,8888660	explorer.exe	3300	Load Image	C:\Windows\System32\version.dll	SUCCESS
20:30:26,8933604	explorer.exe	3300	Load Image	C:\Windows\System32\mswsock.dll	SUCCESS
20:30:26,8949202	explorer.exe	3300	Load Image	C:\Windows\System32\WSH_TCPIP.DLL	SUCCESS
20:30:26,8961519	explorer.exe	3300	Load Image	C:\Windows\System32\wship6.dll	SUCCESS
20:30:26,9097086	explorer.exe	3300	Load Image	C:\Windows\System32\vasadhlp.dll	SUCCESS
20:30:26,9318707	explorer.exe	3300	Load Image	C:\Windows\System32\FWPUCCLNT.DLL	SUCCESS
20:30:26,9340407	explorer.exe	3300	Load Image	C:\Windows\System32\comdlg32.dll	SUCCESS
20:30:26,9422557	explorer.exe	3300	Load Image	C:\Windows\System32\uxtheme.dll	SUCCESS
20:30:26,9535525	explorer.exe	3300	Load Image	C:\Program Files\Internet Explorer\sqmapi.dll	SUCCESS
20:30:26,9757628	explorer.exe	3300	Thread Create		SUCCESS
20:30:26,9770948	explorer.exe	3300	Thread Create		SUCCESS
20:30:26,9795929	explorer.exe	3300	Load Image	C:\Windows\System32\dwmapi.dll	SUCCESS
20:30:26,9957440	explorer.exe	3300	Thread Create		SUCCESS
20:30:27,1159037	explorer.exe	3300	Load Image	C:\Windows\System32\apphelp.dll	SUCCESS
20:30:27,1622701	explorer.exe	3300	Load Image	C:\Windows\System32\vasapi32.dll	SUCCESS
20:30:27,1714814	explorer.exe	3300	Load Image	C:\Windows\System32\vasman.dll	SUCCESS
20:30:27,1721397	explorer.exe	3300	Load Image	C:\Windows\System32\vtutils.dll	SUCCESS
20:30:27,1835143	explorer.exe	3300	Thread Create		SUCCESS
20:30:27,1869287	explorer.exe	3300	Load Image	C:\Windows\System32\SensApi.dll	SUCCESS
20:30:27,1902743	explorer.exe	3300	Load Image	C:\Windows\System32\inlapi.dll	SUCCESS
20:30:27,2001367	explorer.exe	3300	Thread Create		SUCCESS
20:30:27,2041595	explorer.exe	3300	Load Image	C:\Windows\System32\NapiNSP.dll	SUCCESS
20:30:27,2053029	explorer.exe	3300	Process Create	C:\Program Files\Internet Explorer\explorer.exe	SUCCESS
20:30:27,2053093	explorer.exe	3308	Process Start		SUCCESS
20:30:27,2053132	explorer.exe	3308	Thread Create		SUCCESS
20:30:27,2362313	explorer.exe	3300	Load Image	C:\Windows\System32\pnprps.dll	SUCCESS
20:30:27,2394234	explorer.exe	3308	Load Image	C:\Program Files\Internet Explorer\explorer.exe	SUCCESS
20:30:27,2437674	explorer.exe	3308	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS
20:30:27,2477858	explorer.exe	3308	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS