



REPORT

BONUS

Alejandro Cristino
S10 L5



Traccia

BONUS:

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 (no, non ridete ragazzi)

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

Esercizio Traccia e requisiti 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 iexplore è Microsoft quindi è buono, punto.

1. Analisi statica base

Per prima cosa importiamo il nostro file eseguibile iexplore.exe su CFF Explorer, un tool utile che ci permette di visualizzare e modificare dettagliatamente le strutture interne di un file eseguibile.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFFFF	FFFFFFFF	0000F6A8	00009000
KERNEL32.dll	56	0000F728	FFFFFFFF	FFFFFFFF	0000F698	00009070
USER32.dll	9	0000F8F0	FFFFFFFF	FFFFFFFF	0000F68C	00009238
msvcrt.dll	29	0000F940	FFFFFFFF	FFFFFFFF	0000F680	00009288
ntdll.dll	3	0000FA30	FFFFFFFF	FFFFFFFF	0000F674	00009378
SHLWAPI.dll	23	0000FA50	FFFFFFFF	FFFFFFFF	0000F668	00009398
SHELL32.dll	7	0000FB10	FFFFFFFF	FFFFFFFF	0000F65C	00009458
ole32.dll	5	0000FB50	FFFFFFFF	FFFFFFFF	0000F650	00009498
iertutil.dll	14	0000FB80	FFFFFFFF	FFFFFFFF	0000F640	000094C8
urlmon.dll	3	0000FBF8	FFFFFFFF	FFFFFFFF	0000F634	00009540

1. ADVAPI32.dll

- **Descrizione:** Questa DLL fornisce funzioni avanzate di API per Windows, tra cui la gestione della sicurezza, delle chiavi di registro e delle operazioni di logging degli eventi.
- **Numero di funzioni importate:** 13

2. KERNEL32.dll

- **Descrizione:** Questa DLL contiene funzioni core per l'API di Windows, tra cui la gestione della memoria, l'accesso ai file e le operazioni di input/output.
- **Numero di funzioni importate:** 56

3.USER32.dll

- **Descrizione:** Questa DLL include funzioni per la gestione delle finestre e delle interfacce utente, come la gestione delle finestre, le manipolazioni delle GUI e il controllo dell'input dell'utente.
- **Numero di funzioni importate:** 9

4.msvcrt.dll

- **Descrizione:** Questa DLL è la libreria di runtime di Microsoft C, che fornisce funzioni standard del linguaggio C, come la gestione delle stringhe, la gestione della memoria e le operazioni matematiche.
- **Numero di funzioni importate:** 29

5.ntdll.dll

- **Descrizione:** Questa DLL contiene funzioni di basso livello per l'API di Windows NT, che sono utilizzate dal sistema operativo stesso. Include funzioni per la gestione delle eccezioni, delle stringhe, dei processi e delle operazioni di threading.
- **Numero di funzioni importate:** 3

6.SHLWAPI.dll

- **Descrizione:** Questa DLL fornisce funzioni di utilità per semplificare la gestione delle stringhe, le operazioni di file e altre funzioni comuni utilizzate dalle applicazioni di Windows.
- **Numero di funzioni importate:** 23

7.SHELL32.dll

- **Descrizione:** Questa DLL contiene funzioni utilizzate dall'interfaccia grafica di Windows Shell, come l'esplorazione dei file e delle cartelle e l'avvio delle applicazioni.
- **Numero di funzioni importate:** 7

8.ole32.dll

- **Descrizione:** Questa DLL fornisce funzioni per la tecnologia di Object Linking and Embedding (OLE) di Windows, che consente alle applicazioni di creare e manipolare oggetti COM (Component Object Model).
- **Numero di funzioni importate:** 13

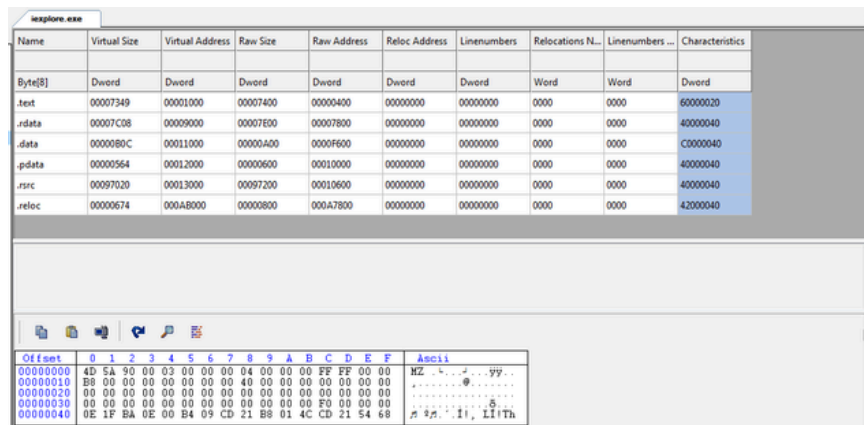
9.iertutil.dll

- **Descrizione:** Questa DLL è associata a Internet Explorer e fornisce funzioni di utilità e supporto per le operazioni di navigazione web e gestione delle risorse di rete.
- **Numero di funzioni importate:** 14

10.urlmon.dll

- **Descrizione:** Questa DLL è utilizzata da Internet Explorer e altre applicazioni per gestire le operazioni di download e manipolazione delle risorse di rete, come gli URL e i protocolli HTTP.
- **Numero di funzioni importate:** 3

Vediamo ora le sezioni, spesso in formato PE (Portable Executable). Queste sezioni sono aree di memoria organizzate all'interno del file e contengono diverse tipologie di dati e istruzioni necessarie per il funzionamento del programma.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00007349	00001000	00007400	00000400	00000000	00000000	0000	0000	60000020
.rdata	00007C08	00009000	00007E00	00007800	00000000	00000000	0000	0000	40000040
.data	0000080C	00011000	00000A00	0000F600	00000000	00000000	0000	0000	C0000040
.pdata	00000564	00012000	00000600	00010000	00000000	00000000	0000	0000	40000040
.rsrc	00007020	00013000	00007200	00010600	00000000	00000000	0000	0000	40000040
.reloc	00000674	000A8000	00000800	000A7800	00000000	00000000	0000	0000	42000040

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	HZ 99 . .
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00S.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00i.i.i
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68LiTh

- 1).text
 - Descrizione: Questa sezione contiene il codice eseguibile del programma. È una delle sezioni più importanti perché contiene le istruzioni che verranno eseguite dalla CPU.
- 2).rdata
 - Descrizione: Questa sezione contiene dati di sola lettura, come stringhe di testo, informazioni di debug e altre costanti che il programma utilizza durante l'esecuzione.
- 3).data
 - Descrizione: Questa sezione contiene dati di lettura e scrittura, come variabili globali e dati inizializzati.
- 4).pdata
 - Descrizione: Questa sezione contiene informazioni sulle procedure utilizzate dal programma, come i gestori delle eccezioni.
- 5).rsrc
 - Descrizione: Questa sezione contiene risorse utilizzate dal programma, come immagini, icone, e menu.
- 6).reloc
 - Descrizione: Questa sezione contiene informazioni di rilocalizzazione che vengono utilizzate per correggere gli indirizzi del codice quando il file eseguibile viene caricato in memoria.

Conclusioni

Sulla base delle informazioni estratte dalle analisi del file "iexplore.exe", possiamo ragionevolmente concludere che il file in esame non mostra segni di essere un malware. Le importazioni di moduli e la struttura delle sezioni sono conformi a quelle di un'applicazione legittima, in questo caso Internet Explorer. Tuttavia, per una valutazione definitiva e completa, sarebbe utile eseguire ulteriori analisi dinamiche

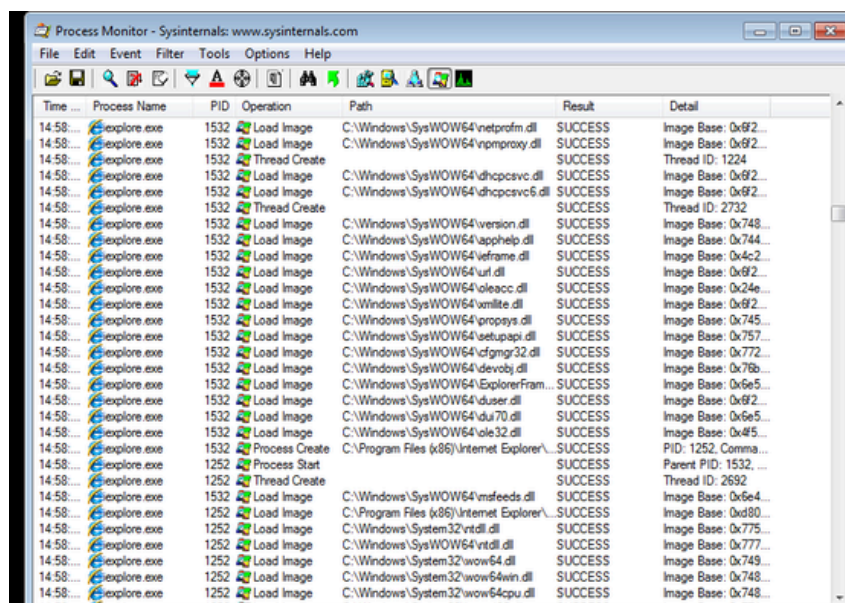
2. Analisi dinamica base

Dopo l'analisi statica effettuata, proseguiamo con un'analisi dinamica del file in questione per capirne in maniera più approfondita il funzionamento.

Avviamo Procmon e Regshot prima di eseguire iexplore.exe.

facciamo partire Regshot con il primo shot, successivamente avviamo il file ed eseguiamo il secondo shot

Il filtro processi e thread



Time ...	Process Name	PID	Operation	Path	Result	Detail
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\netprofm.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\vpnmproxy.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Thread Create		SUCCESS	Thread ID: 1224
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Thread Create		SUCCESS	Thread ID: 2732
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\version.dll	SUCCESS	Image Base: 0x748...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x744...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\eframe.dll	SUCCESS	Image Base: 0x4c2...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\url.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\oleacc.dll	SUCCESS	Image Base: 0x24e...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\wmilte.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\propsys.dll	SUCCESS	Image Base: 0x745...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\setupapi.dll	SUCCESS	Image Base: 0x757...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\cfgmgr32.dll	SUCCESS	Image Base: 0x772...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Image Base: 0x76b...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\ExplorerFrame...	SUCCESS	Image Base: 0x6e5...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\duser.dll	SUCCESS	Image Base: 0x92...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\dui70.dll	SUCCESS	Image Base: 0x6e5...
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x4f5...
14:58:...	iexplore.exe	1532	Process Create	C:\Program Files (x86)\Internet Explorer\...	SUCCESS	PID: 1252, Comma...
14:58:...	iexplore.exe	1252	Process Start		SUCCESS	Parent PID: 1532, ...
14:58:...	iexplore.exe	1252	Thread Create		SUCCESS	Thread ID: 2692
14:58:...	iexplore.exe	1532	Load Image	C:\Windows\SysWOW64\msfeeds.dll	SUCCESS	Image Base: 0x6e4...
14:58:...	iexplore.exe	1252	Load Image	C:\Program Files (x86)\Internet Explorer\...	SUCCESS	Image Base: 0xd80...
14:58:...	iexplore.exe	1252	Load Image	C:\Windows\System32\rtldll.dll	SUCCESS	Image Base: 0x775...
14:58:...	iexplore.exe	1252	Load Image	C:\Windows\SysWOW64\rtldll.dll	SUCCESS	Image Base: 0x777...
14:58:...	iexplore.exe	1252	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x749...
14:58:...	iexplore.exe	1252	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x748...
14:58:...	iexplore.exe	1252	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x748...

Prima Immagine: Il filtro sui processi e thread

L'immagine mostra il monitoraggio dei processi e dei thread creati e gestiti da "iexplore.exe". Qui ci sono alcune osservazioni principali:

- **Process Name:** iexplore.exe
- **PID (Process ID):** Vari processi con ID come 1532, 1528, ecc.
- **Operations:** Load Image, Thread Create, Process Create.
- **Path:** Molti dei percorsi indicano DLL di sistema come C:\Windows\SysWOW64\ntdll.dll, C:\Windows\SysWOW64\kernel32.dll, ecc.
- **Result:** SUCCESS, che indica che le operazioni sono state completate con successo.

Questa immagine mostra che "iexplore.exe" carica una serie di librerie di sistema necessarie per il suo funzionamento e crea nuovi thread e processi in modo legittimo.

Il filtro file system

Process Monitor - Sysinternals: www.sysinternals.com

File Edit View Filter Tools Options Help

Time	Process Name	PID	Operation	Path	Result	Detail
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	FileSystemControl	C:\Users\user\AppData\Roaming\Micro...	NOT REPARSE P...	Control: FSCTL_G...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	DeviceIoControl	C:\Users\user\AppData\Roaming\Micro...	INVALID PARAME...	Control: IOCTL_M...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	FileSystemControl	C:\Users\user\AppData\Roaming\Micro...	NOT REPARSE P...	Control: FSCTL_G...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	IS DIRECTORY	Desired Access: R...
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	FileSystemControl	C:\Users\user\AppData\Roaming\Micro...	NOT REPARSE P...	Control: FSCTL_G...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	DeviceIoControl	C:\Users\user\AppData\Roaming\Micro...	INVALID PARAME...	Control: IOCTL_M...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	FileSystemControl	C:\Users\user\AppData\Roaming\Micro...	NOT REPARSE P...	Control: FSCTL_G...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	CloseFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	
14:58	explore.exe	1532	CreateFile	C:\Users\user\AppData\Roaming\Micro...	SUCCESS	Desired Access: R...
14:58	explore.exe	1532	DeviceIoControl	C:\Users\user\AppData\Roaming\Micro...	INVALID PARAME...	Control: IOCTL_M...

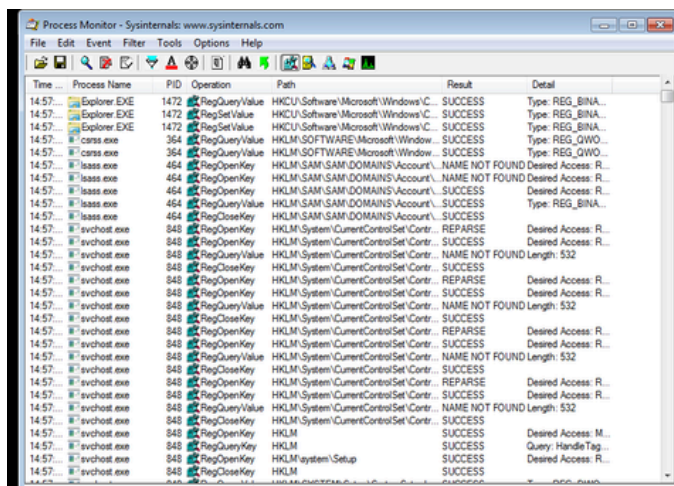
Seconda Immagine: Il filtro file system

Questa immagine mostra le operazioni del file system eseguite da "iexplore.exe". Ecco alcuni dettagli:

- **Process Name:** iexplore.exe
- **PID (Process ID):** Principalmente 1532.
- **Operations:** CreateFile, CloseFile, FileSystemControl, DeviceControl.
- **Path:** Molti percorsi indicano directory sotto C:\Users\user\AppData\Roaming\Microsoft\.
- **Result:** SUCCESS, NOT REPARSE POINT, DIRECTORY, INVALID PARAMETER, ecc.

Le operazioni di "iexplore.exe" sul file system sembrano legittime e riguardano la creazione, l'apertura e la chiusura di file nelle directory di dati utente, tipicamente utilizzate da un browser per memorizzare configurazioni e dati temporanei.

Il filtro attività sul registro



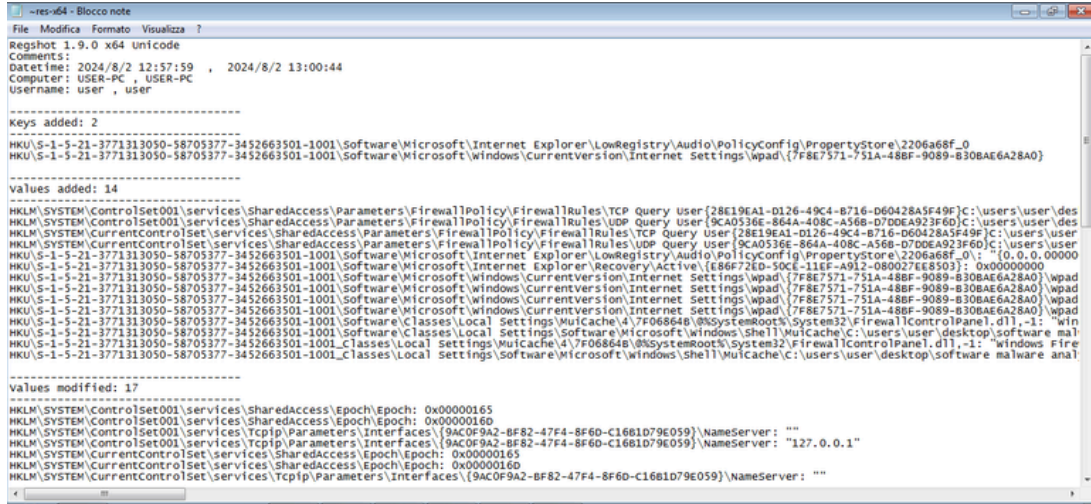
Terza Immagine: Il filtro attività sul registro

Questa immagine mostra le attività di registro eseguite da "iexplore.exe" e altri processi come svchost.exe e lsass.exe. Ecco i dettagli:

- **Process Name:** iexplore.exe, svchost.exe, lsass.exe.
- **PID (Process ID):** 1472, 464, 848, ecc.
- **Operations:** RegQueryValue, RegSetValue, RegOpenKey, RegCloseKey.
- **Path:** Vari percorsi nel registro, come HKCU\Software\Microsoft\Windows\..., HKLM\SAM\..., ecc.
- **Result:** SUCCESS, NAME NOT FOUND, REPARSE.

Le operazioni di registro eseguite da "iexplore.exe" e altri processi sono legittime attività di configurazione e gestione delle impostazioni del sistema operativo e delle applicazioni.

Confronto Regshot



Quarta Immagine: Confronto Regshot

L'analisi con Regshot mostra le modifiche al registro di sistema tra due snapshot presi prima e dopo l'esecuzione di "iexplore.exe":

1.Chiavi Aggiunte:

- Due chiavi aggiunte relative alle impostazioni delle connessioni di rete di Internet Explorer:
 - HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\LowRegistry\Audio\PolicyConfig\PropertyStore\2206a68f_0
 - HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Wpad\{F8E7571F-751A-48BF-9089-B30BAE6A28A0}

2.Valori Aggiunti:

- **14 valori aggiunti principalmente legati alle impostazioni del firewall e alle configurazioni di rete.**

3.Valori Modificati:

- 17 valori modificati che riguardano le impostazioni del servizio di rete e del firewall, come:
 - HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules
 - HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces

3. Risposta alla segnalazione del dipendente

Sulla base delle analisi delle sezioni del file, delle importazioni, delle attività di sistema monitorate con Procmon e delle modifiche al registro rilevate con Regshot, posso concludere che "iexplore.exe" mostra comportamenti tipici di un browser web legittimo. Le operazioni eseguite dal file sono coerenti con quelle necessarie per il funzionamento di Internet Explorer e non presentano segni di attività malevola.

Punti Chiave:

- **Importazioni Legittime:** I moduli importati sono tutti DLL standard di Windows.
- **Struttura del File:** Le sezioni del file sono in linea con quelle di un eseguibile legittimo.
- **Attività di Sistema:** Le operazioni di processo, file system e registro non mostrano anomalie o comportamenti sospetti.
- **Modifiche al Registro:** Le modifiche sono coerenti con le normali operazioni di un browser, come aggiornamenti delle impostazioni di rete e del firewall.

In conclusione, sulla base delle evidenze raccolte, come membro senior del SOC posso affermare e assicurare il dipendente che con ragionevole certezza "iexplore.exe" non è un malware, ma un componente legittimo del sistema operativo Windows.

