

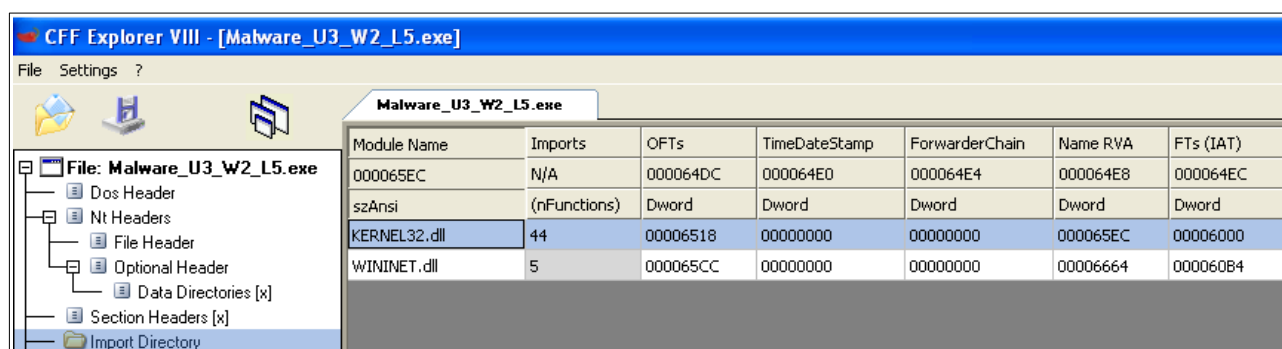
Analisi Statica e Costrutti di un Codice

Obiettivo: Analizzare un Malware e un codice dati dalla traccia.

1) Analisi Statica di un Malware (Librerie)

L'esercizio ci chiede per prima cosa di analizzare le *Librerie* di un **Malware** presente all'interno della macchina **Malware Analysis_Final**. Avvio la macchina e dato che le librerie di un **Malware** si possono controllare con un'*Analisi Statica Basica* in questo caso non c'è bisogno di controllare se siamo "offline" o separati dalla macchina **Host**.

Per l'analisi mi sono avvalso del programma **CFF Explorer**, un tool che viene utilizzato per esplorare ed analizzare file eseguibili, è di aiuto in questo punto per elencare le librerie importate dal **Malware** e nel prossimo per controllare le *Sezioni* che vanno a comporre lo stesso.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000065EC	N/A	000064DC	000064E0	000064E4	000064E8	000064EC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

Possiamo vedere che le *Librerie* importate dall'eseguibile sono:

- **KERNEL32.dll**: una libreria comune che contiene le funzioni principali per interagire con il sistema operativo. Ad esempio manipolazione dei file e gestione della memoria. La libreria in questo caso importa 44 funzioni.
- **WININET.dll**: questa libreria contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP ed NTP.

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00006640	00006640	0071	InternetOpenUrlA
0000662A	0000662A	0056	InternetCloseHandle
00006616	00006616	0077	InternetReadFile
000065FA	000065FA	0066	InternetGetConnectedState
00006654	00006654	006F	InternetOpenA

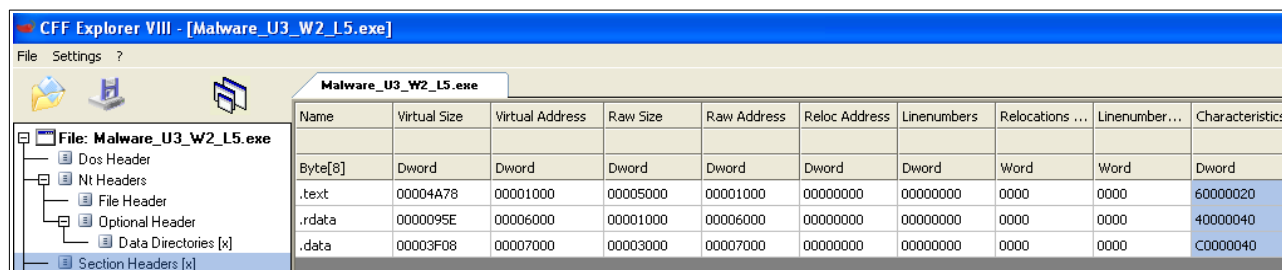
Possiamo notare che tra le funzioni importate da **WININET** sono presenti alcune che portano il **Malware** a collegarsi ad un dato **URL (InternetOpenUrlA)** e a stabilire una sessione di connessione, che può essere tramite protocollo **FTP** o **HTTP (InternetOpenA)**.

Quindi il **Malware** richiama tali funzioni contenute nelle librerie per poter svolgere i compiti per il quale è stato programmato.

2) Analisi Statica di un Malware (Sezioni)

Secondo punto dell'esercizio è identificare le *Sezioni* dello stesso **Malware**.

Le *Sezioni* del **Malware** analizzato come detto in precedenza possono essere visualizzate con lo stesso tool **CFF Explorer** in *Section Headers* sulla sinistra.



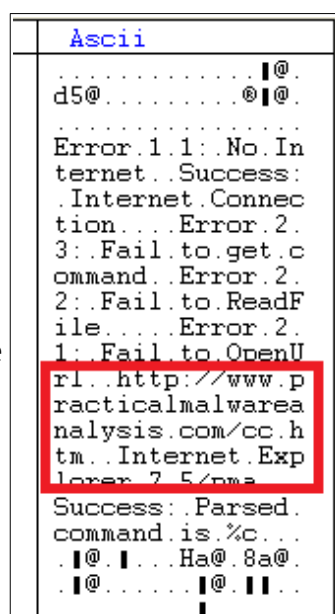
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

Ogni sezione ha un preciso scopo e in questo caso sono presenti:

- **.text**: contiene istruzioni (righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Questa sezione viene eseguita dalla CPU.
- **.rdata**: include informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.
- **.data**: questa sezione contiene i dati e variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Spulciando la sezione **.data** si può trovare un URL.

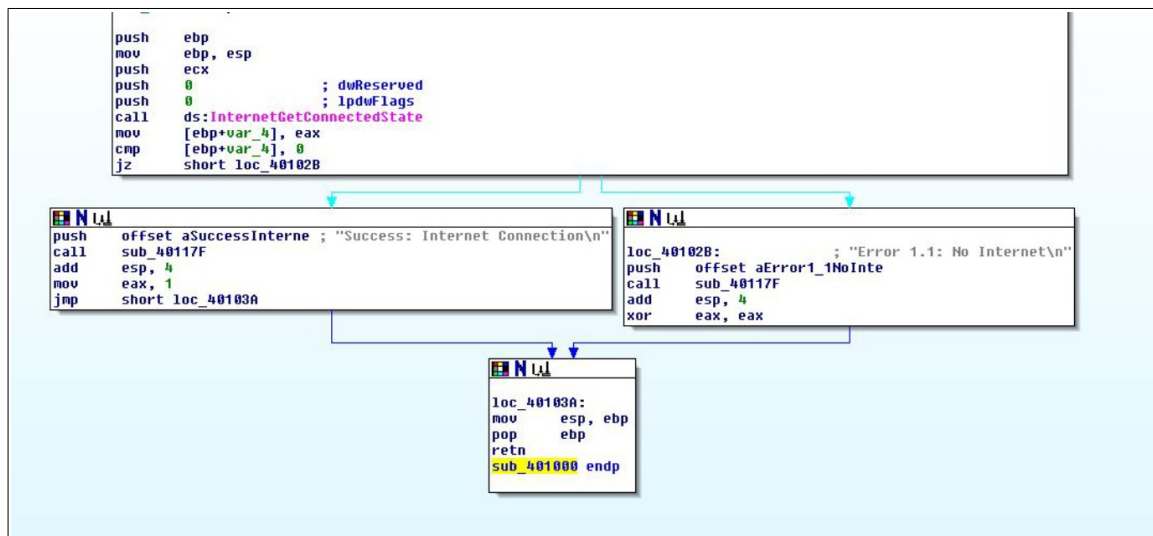
Riprendendo le funzioni della libreria **WININET** analizzate prima suppongo che sia il sito dove il **Malware** vada a creare una sessione di connessione.



```
Ascii
.....!@.
d5@.....!@.
.....
Error.1.1:..No.In
ternet..Success:
..Internet.Connec
tion....Error.2.
3:..Fail.to.get.c
ommand..Error.2.
2:..Fail.to.ReadF
ile....Error.2.
1:..Fail.to.OpenU
rl..http://www.p
racticalmalwarea
nalysis.com/cc.h
tm..Internet.Exp
lorer.7.5/pma
Success:..Parsed.
command.is.%c...
..!@.!!..Ha@.8a@.
..!@.....!@.!!..
.....!.....
```

3) Costrutti di un Codice

Il terzo punto dell'esercizio chiede di identificare i *Costrutti* di codice **Assembly** del seguente codice



Primo Costrutto: Creazione dello Stack.

```
push    ebp
mov     ebp, esp
```

Secondo Costrutto: Chiamata Funzione InternetGetConnectedState.

```
push    ecx
push    0
push    0
call    ds:InternetGetConnectedState
```

Terzo Costrutto: Ciclo IF dove se ZF è 1 (ovvero se il valore di [ebp+var_4] è 0) salta alla locazione di memoria indicata (loc_40102B).

```
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

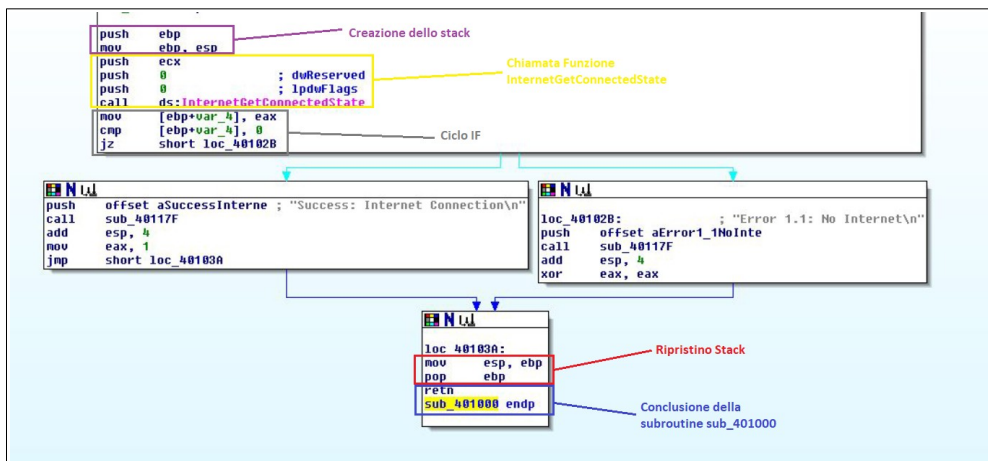
Quarto Costrutto: Rispristino dello Stack

```
mov     esp, ebp
pop     ebp
```

Quinto Costrutto: Conclusione della subroutine sub_401000, inoltre non essendoci un numero accanto si presuppone che non vi siano byte da rimuovere.

```
retn
sub_401000 endp
```

Per concludere il punto ho modificato l'immagine originale indicando i vari *Costrutti*.



4) Ipotizzare il Comportamento del Codice

La quarta richiesta della traccia è quella di ipotizzare cosa questo codice faccia.

Per prima cosa il codice mostrato crea lo *stack* per gestire le informazioni durante la sua esecuzione. Successivamente richiama la funzione **InternetGetConnectedState** per determinare lo stato della connessione del **Sistema Operativo**. Questa funzione infatti fa parte della libreria **WININET** e richiede l'utilizzo di due argomenti (in questo caso i due *push 0* rispettivamente *dwReserved* e *lpdwflags*).

Successivamente viene indotto un ciclo IF dove assegnando il valore di *eax* alla variabile `[ebp+var_4]`, essa viene messa in comparazione con il valore 0. Il *Jump jz* serve ad indicare che se il valore di **Sorgente** e **Destinazione** sono uguali (ovvero se la variabile è 0 e quindi $ZF = 1$) la funzione esegue un salto alla locazione indicata (`loc_40102B`).

Nel caso venga eseguito il salto:

se il salto viene effettuato il codice inserisce all'interno dello *stack* la stringa di testo `aError1_1NoInte` (presumibilmente assenza di internet o una connessione non riuscita) chiamando una subroutine (`sub_40117F`), ripristinando l'indicatore dello *stack* con l'aggiunta di 4 byte e infine azzerare con l'operatore logico *XOR* il registro *eax*.

Nel caso Non venga eseguito il salto:

se il salto **Non** viene effettuato allora il codice procede con l'inserire una stringa di testo `aSuccessInterne` (quindi questa volta la connessione è presente) richiamando la subroutine precedente (che viene eseguita indipendentemente dalla verifica della condizione IF ma per saperne di più servirebbe il resto del codice), ripristinando l'indicatore dello *stack* con i 4 byte e il valore del registro *eax* ad 1. Infine esegue un *Salto Incondizionato* alla locazione `40103A`.

Questa locazione indica la fine di una subroutine (`sub_401000`) diversa da quella indicata precedentemente dove possiamo notare il *Ripristino dello Stack* e la sua conclusione effettiva con *retn* e *endp*.

In conclusione: il codice controlla quindi lo stato della **Connessione Internet** e in entrambi i casi salva una stringa di testo che andrà probabilmente ad essere "stampata" alla subroutine `40117F` dove suppongo sia indicata la funzione *Printf* presente in entrambe le possibilità del **Ciclo IF** (ovvero Connessione presente e Non).

Bonus) Internet Explorer

Come bonus la traccia ci chiede di controllare che il file “sospetto” **IEXPLORER.EXE** non sia maligno su segnalazione di un dipendente. In primo luogo se il dipendente non conoscesse **Internet Explorer** (per fare questa bizzarra segnalazione) gli chiederei dove viva per non conoscere il “miglior browser per scaricare altri browser”, ma a parte gli scherzi per controllare se il file sia o meno malevolo ho iniziato l’analisi controllando l’*hash* con **md5deep** da riga di comando.

```
C:\> Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd Desktop\md5deep-4.3

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "c:\Program
Files\Internet Explorer\IEXPLORE.EXE"
55794b97a7faabd2910873c85274f409 c:\Program Files\Internet Explorer\IEXPLORE.E
X

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>_
```

Una volta ottenuta l’ho caricata su **VirusTotal** ed è venuto fuori che effettivamente si tratta di un file sicuro come mostrano le immagini sotto.

Basic properties

MD5	55794b97a7faabd2910873c85274f409
SHA-1	58e80c90bf54850b5f3ccbd8edf0877537e0ea8e
SHA-256	814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e
Vhash	0940366d155az2b01gz11z1fz1
Authenthash	f173fd99db212a5c686a123f32d2de6ce8a8f3699aea14a986a23ce5c125a263
Imphash	b06090332cc8fb8aeb9b846fd7ff33c
Rich PE header hash	acd22b07f3aa1c5ecfa9d8f4a53a0ba
SSDEEP	1536:PgkhByl4BcDQX2ooD+AyxAIVJ9bayZbScKcEang5Kmp:xe146QXmmAIX1tanUKmp
TLSH	T18E93B252FA14ED61CA9C08305867CBA41820BC72DB119BE776F0BB1FAD363D37A3
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) Win64 Executable (generic) (15.9%) Win32 Dynamic Link Library (generic) (9.9%) Win16 NE executable (generic) (7.6%) Win32 Executable (generic) (5.8%)
DetectItEasy	PE32 Compiler: EP Microsoft Visual C/C++ (2005) [EXE32] Compiler: Microsoft Visual C/C++ (2003) Linker: Microsoft Linker (7.10*) [GUI32]
File size	91.00 KB (93184 bytes)

0 / 71

File distributed by Microsoft

814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e

IEXPLORE.EXE

Size 91.00 KB

peexe known-distributor trusted

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 15

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	ALYac	Undetected
Antiy-AVL	Undetected	Arcabit	Undetected

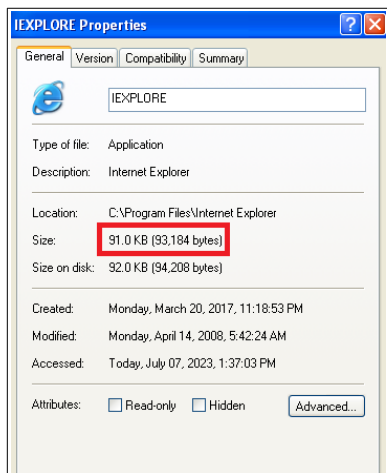
Sembrerebbe che sia tutto nella norma ma il famoso dipendente non si fida affatto perciò ho controllato con il tool **strings** se ci fossero stringhe di codice che ci indicassero qualcosa di particolare, ad esempio trattandosi di **Internet Explorer** stringhe che riguardassero una connessione a siti malevoli o creazioni di *backdoor*.

A parte una serie di stringhe incomprensibili l’unica cosa interessante è la parte finale che ci mostra effettivamente che si tratta di un File Originale di Microsoft con tanto di **Versione e Diritti Riservati**.

Il resto delle stringhe non sembrano di particolare rilevanza nel cercare un possibile **Malware** perciò da questo punto di vista il File sembra essere sano.

```
US_VERSION_INFO
StringFileInfo
040904B0
CompanyName
Microsoft Corporation
FileDescription
Internet Explorer
FileVersion
6.00.2900.5512 <xpsp.080413-2105>
InternalName
iexplore
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
IEXPLORE.EXE
ProductName
Microsoft
Windows
Operating System
ProductVersion
6.00.2900.5512
0c0904E4
CompanyName
Microsoft Corporation
FileDescription
Internet Explorer
FileVersion
6.00.2900.5512
InternalName
iexplore
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
IEXPLORE.EXE
ProductName
Microsoft
Windows
Operating System
ProductVersion
6.00.2900.5512
VarFileInfo
Translation
1
This is being run in compatibility mode and not all features are enabled.$Inter
net Explorer Compatibility mode
Internet Explorer
```

Un'ulteriore prova è la grandezza del file, se ci sono state manomissioni il file all'interno della macchina i suoi byte saranno diversi da quelli di un file tipico di **Microsoft**. **VirusScan** indica che la grandezza del file dovrebbe essere *93184 bytes* e andando sulle proprietà del file analizzato possiamo vedere che è la stessa grandezza.



Per continuare l'analisi imposta dal dipendente sospettato ho avviato **CFF Explorer** per cercare più a fondo.

Le librerie importate sembrano essere quelle standard di **Internet Explorer** senza nessuna aggiunta, ad esempio una libreria che possa importare funzioni per protocolli **HTTP** o **FTP** come può essere **WININET**.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
msvcrt.dll	1	00002830	FFFFFFFF	FFFFFFFF	0000284C	00001144
KERNEL32.dll	43	000026EC	FFFFFFFF	FFFFFFFF	00002B66	00001000
USER32.dll	16	000027EC	FFFFFFFF	FFFFFFFF	00002C8C	00001100
SHLWAPI.dll	16	000027A8	FFFFFFFF	FFFFFFFF	00002D30	000010BC
SHDOCVW.dll	2	0000279C	FFFFFFFF	FFFFFFFF	00002D3C	000010B0

Le librerie “nuove” che vediamo riguardano principalmente la gestione di interfaccia utente (**USER32**), offrire supporto per la navigazione web (**SHDOCVW**) e per operazioni di basso livello (**SHLWAPI**).

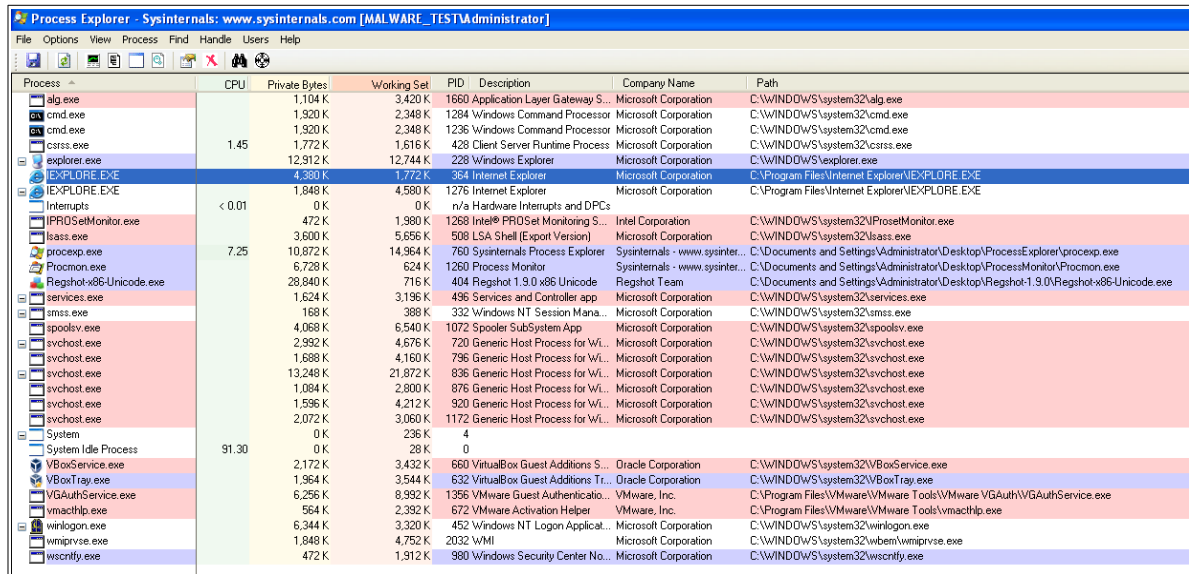
Per quanto riguarda l'analisi statica di questo file “sospetto” possiamo affermare che non ci siano problemi di nessun tipo, il file sembra apposto, ma per evitare che il famoso dipendente possa telefonarmi nel cuore della notte in preda alla paranoia decido di effettuare un' **Analisi Dinamica**, ovvero avviare il “**Malware**” in ambiente protetto.

Decido quindi di avviare innanzitutto **Process Explorer**, molto utile perchè nel caso Internet Explorer apra nuovi processi verranno visualizzati sulla GUI del tool, **Procmon**, con la quale posso visualizzare eventuali modifiche apportate, ad esempio al *File System*, ed infine **Regshot**, tool molto utile per confrontare eventuali modifiche ai Registri di Sistema.

L'avvio di Internet Explorer l'ho eseguito completamente *offline*, cioè con scheda di rete e cartelle di condivisione disabilitate. Per cominciare ho avviato i tre tool e ho cominciato creando lo “snapshot” del **Registro** prima dell'avvio di IE.

Process Explorer

All'avvio di Internet Explorer ho controllato la GUI del tool per cercare processi sospetti; per facilitare la ricerca ho aggiunto come colonna il Path dei programmi avviati, indicandomi quindi da dove venissero eseguiti.

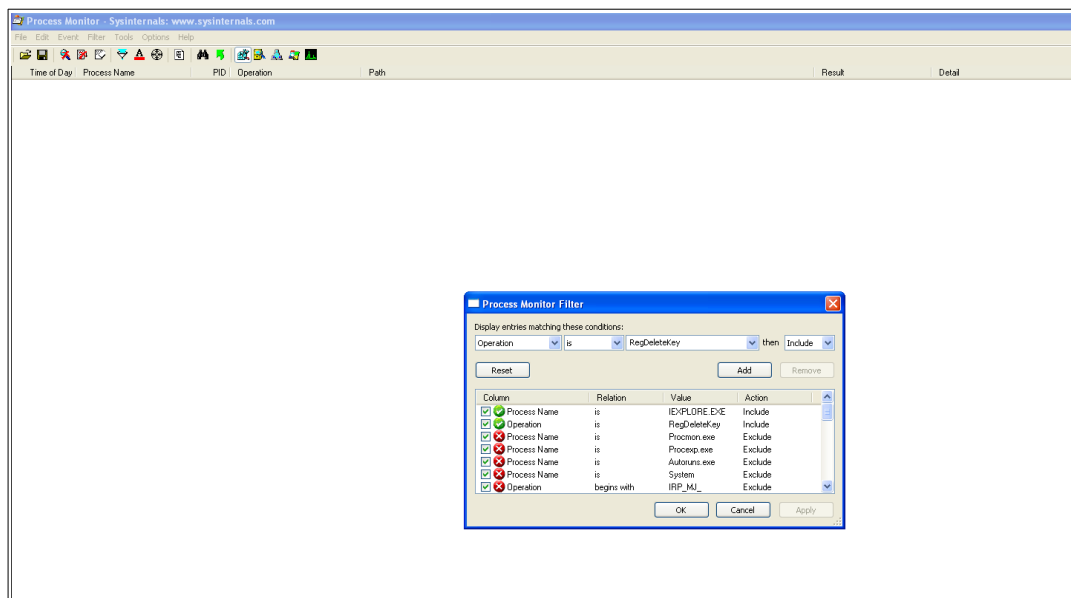


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Path
alg.exe		1,104 K	3,420 K	1660	Application Layer Gateway S...	Microsoft Corporation	C:\WINDOWS\system32\alg.exe
cmd.exe		1,920 K	2,348 K	1284	Windows Command Processor	Microsoft Corporation	C:\WINDOWS\system32\cmd.exe
csrss.exe		1,920 K	2,348 K	1236	Windows Command Processor	Microsoft Corporation	C:\WINDOWS\system32\cmd.exe
csrss.exe		1,772 K	1,616 K	428	Client Server Runtime Process	Microsoft Corporation	C:\WINDOWS\system32\csrss.exe
explorer.exe	1.45	12,912 K	12,744 K	228	Windows Explorer	Microsoft Corporation	C:\WINDOWS\explorer.exe
EXPLORE.EXE		4,380 K	1,772 K	364	Internet Explorer	Microsoft Corporation	C:\Program Files\Internet Explorer\EXPLORE.EXE
EXPLORE.EXE		1,848 K	4,580 K	1276	Internet Explorer	Microsoft Corporation	C:\Program Files\Internet Explorer\EXPLORE.EXE
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs		
IPROSetMonitor.exe		472 K	1,980 K	1268	Intel® PROSet Monitoring S...	Intel Corporation	C:\WINDOWS\system32\IPROSetMonitor.exe
lsass.exe		3,600 K	5,656 K	508	LSA Shell (Export Version)	Microsoft Corporation	C:\WINDOWS\system32\lsass.exe
procexp.exe	7.25	10,872 K	14,964 K	760	Sysinternals Process Explorer	Sysinternals - www.sysinter...	C:\Documents and Settings\Administrator\Desktop\Process Explorer\procexp.exe
Procmon.exe		6,728 K	624 K	1260	Process Monitor	Sysinternals - www.sysinter...	C:\Documents and Settings\Administrator\Desktop\Process Monitor\Procmon.exe
Regshot-x86-Unicode.exe		28,840 K	716 K	404	Regshot 1.9.0 x86 Unicode	Regshot Team	C:\Documents and Settings\Administrator\Desktop\Regshot-1.9.0\Regshot-x86-Unicode.exe
services.exe		1,624 K	3,196 K	496	Services and Controller app	Microsoft Corporation	C:\WINDOWS\system32\services.exe
smss.exe		168 K	388 K	332	Windows NT Session Mana...	Microsoft Corporation	C:\WINDOWS\system32\smss.exe
spoolsv.exe		4,068 K	6,540 K	1072	Spooler SubSystem App	Microsoft Corporation	C:\WINDOWS\system32\spoolsv.exe
svchost.exe		2,992 K	4,676 K	720	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe		1,688 K	4,160 K	796	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe		13,248 K	21,872 K	836	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe		1,084 K	2,800 K	876	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe		1,596 K	4,212 K	920	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
svchost.exe		2,072 K	3,060 K	1172	Generic Host Process for Wl...	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe
System		0 K	236 K	4			
System Idle Process	91.30	0 K	28 K	0			
VBService.exe		2,172 K	3,432 K	660	VirtualBox Guest Additions S...	Oracle Corporation	C:\WINDOWS\system32\VBService.exe
VBTray.exe		1,964 K	3,544 K	632	VirtualBox Guest Additions Tr...	Oracle Corporation	C:\WINDOWS\system32\VBTray.exe
VGAuthService.exe		6,256 K	8,992 K	1356	VMware Guest Authentication...	VMware, Inc.	C:\Program Files\VMware\VMware Tools\VGAuthService.exe
vmacthlp.exe		564 K	2,392 K	672	VMware Activation Helper	VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmacthlp.exe
winslogon.exe		6,344 K	3,320 K	452	Windows NT Logon Applicat...	Microsoft Corporation	C:\WINDOWS\system32\winslogon.exe
wsmprvse.exe		1,848 K	4,752 K	2032	WMI	Microsoft Corporation	C:\WINDOWS\system32\wbem\wsmprvse.exe
wscntfy.exe		472 K	1,912 K	980	Windows Security Center No...	Microsoft Corporation	C:\WINDOWS\system32\wscntfy.exe

Notiamo che i due processi **EXPLORE.EXE** sono entrambi eseguiti dalla Directory giusta.

Process Monitor

ProcMon esegue una scansione continua sul Sistema finché non lo si stoppa. Una volta fermato ho cercato con un filtro il nome del processo desiderato per controllare eventuali criticità e modifiche particolari.



Ad esempio qui ho cercato se il processo abbia eliminato delle Chiavi di Registro; la schermata bianca indica che non è avvenuta tale operazione. Su questo tool ho voluto concentrarmi maggiormente su eventuali modifiche al *File System* e sull'analisi di *Thread*.

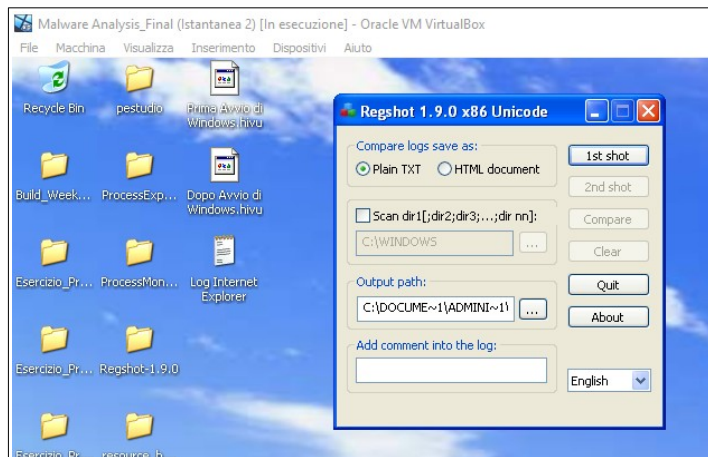
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1/16/16 29562	EXPLORE.DDE	364	C:\CreateFile	C:\	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29566	EXPLORE.DDE	364	C:\QueryDirectory	C:\	SUCCESS	D:\656d5c3a074400905d5a0eb7a\1. AUTODIAG-BAT, FileInformationClass: FileInformation, 3 CONFIG.SYS, 4 Documents and Settings
1/16/16 29577	EXPLORE.DDE	364	C:\QueryDirectory	C:\	NO MORE FILES	
1/16/16 29596	EXPLORE.DDE	364	C:\CloseFile	C:\	SUCCESS	
1/16/16 29598	EXPLORE.DDE	364	C:\CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29602	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 All Users, 4 Default User, 5 LocalizedSVC, 6 NetworkService
1/16/16 29618	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings	NO MORE FILES	
1/16/16 29629	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings	SUCCESS	
1/16/16 29637	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29701	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 Cookies, 4 Desktop, 5 Favorites, 6 Local Settings, 7 My Documents, 8 NetHood
1/16/16 29711	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
1/16/16 29723	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
1/16/16 29738	EXPLORE.DDE	364	C:\CreateFile	C:\Documents and Settings\Administrator\cookies	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29765	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	D:\1...FileInformationClass: FileInformation, 3
1/16/16 29765	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\cookies	NO MORE FILES	
1/16/16 29777	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\cookies	SUCCESS	
1/16/16 29793	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Favorites	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29797	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Favorites	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 Links
1/16/16 29806	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Favorites	NO MORE FILES	
1/16/16 29808	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Favorites	SUCCESS	
1/16/16 29849	EXPLORE.DDE	364	C:\CreateFile	C:\Documents and Settings\Administrator\Local Settings	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29863	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 desktop.ini, 4 History, 5 Temp, 6 Temporary Internet Files
1/16/16 29865	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings	NO MORE FILES	
1/16/16 29872	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Local Settings	SUCCESS	
1/16/16 29890	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29899	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 History\IE
1/16/16 29917	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History	NO MORE FILES	
1/16/16 29924	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Local Settings\History	SUCCESS	
1/16/16 29938	EXPLORE.DDE	364	C:\CreateFile	C:\Documents and Settings\Administrator\Local Settings\History\History\IE	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 29972	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History\History\IE	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 index.dat, 4 MSHTML0120230708\02230707
1/16/16 29985	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History\History\IE	NO MORE FILES	
1/16/16 30003	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Local Settings\History\History\IE	SUCCESS	
1/16/16 30009	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\History\History\IE	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 30044	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 desktop.ini, 3
1/16/16 30044	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	NO MORE FILES	
1/16/16 30072	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
1/16/16 30091	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content\IE5	SUCCESS	D:\1...FileInformationClass: FileInformation, 3
1/16/16 30100	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content\IE5	SUCCESS	D:\1...FileInformationClass: FileInformation, 3 desktop.ini, 4 index.dat
1/16/16 30100	EXPLORE.DDE	364	C:\QueryDirectory	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content\IE5	NO MORE FILES	
1/16/16 30153	EXPLORE.DDE	364	C:\CloseFile	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content\IE5	SUCCESS	
1/16/16 30179	EXPLORE.DDE	364	C:\CreateFile	C:\Documents and Settings\VAL\USERS	SUCCESS	Desired Access: Read Data/Local Directory, Synchronize

Con una rapida occhiata e osservando la figura in alto dal punto di vista dei *File System* non ho trovato particolari modifiche a parte file che riguardano *File Temporanei*, *Cookie* e altro.

Process Monitor - Sysinternals... sysinternals.com						
File Edit View Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
1:16:16.27882	EXPLORE.EXE	364	Process Start		SUCCESS	PowerPID: 228; Command Line: "C:\Program Files\Internet Explorer\EXPLORE.EXE"; Current directory: C:\Program Files\Internet Explorer\
1:16:16.27882	EXPLORE.EXE	364	Thread Create		SUCCESS	ThreadID: 1768
1:16:16.27945	EXPLORE.EXE	364	Load Image	C:\Program Files\Internet Explorer\EXPLORE.EXE	SUCCESS	Image Base: 0x400000; Image Size: 0x1900
1:16:16.27996	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.57021	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.58000	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59125	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.58438	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.58473	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59005	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59069	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59174	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59187	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59188	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.59878	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.62065	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.63017	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.63085	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.64042	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.64139	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.64378	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.62011	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.62012	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.62065	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.63024	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.63088	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.67002	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.67002	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.74984	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.79119	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.84744	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.85200	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.86824	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.86909	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.86982	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.87142	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.90166	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92324	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x760000; Image Size: 0x4000
1:16:16.92325	EXPLORE.EXE	364	Load Image	C:\WINDOWS\system32\ole32.dll		

Per quanto riguarda i *Thread* e *Processi* ugualmente non ho riscontrato particolari irregolarità da parte del Programma Avviato. In alto possiamo vedere che vengono importate le varie librerie e basta.

L'ultimo controllo che ho fatto è aver creato un secondo "snapshot" dei registri con **Regshot** Dopo l'avvio di **Internet Explorer**.



Ho utilizzato l'opzione "Compare" del tool per appunto confrontare i due snapshot per eventuali differenze effettuate ai **Registri**.

[illegible]

Possiamo notare che tra le **Chiavi di Registro** aggiunte, modificate o eliminate ci sono principalmente a **ProcMon** e a **Process Explorer**; non ci sono valori critici o modifiche significative che possano far pensare ad un **Malware** o alla modifica dell'eseguibile di **Internet Explorer** con tool appositi come ad esempio **Msfvenom**.

In conclusione posso affermare che il file eseguibile **IEXPLORER.EXE** sia un file di **Windows** innocuo, ciò non toglie che il supporto a **Internet Explorer** è innanzitutto terminato a Giugno del 2022, perciò bisognerebbe optare per l'utilizzo di un altro **Browser** (ad esempio **Firefox**, **Chrome** o **Edge**, il nuovo Browser di Microsoft).

PS: a meno che non ci siano sorprese riguardanti il file sopracitato, se il dipendente continua ad essere sospettoso chiudetelo in uno scantinato e buttate la chiave.