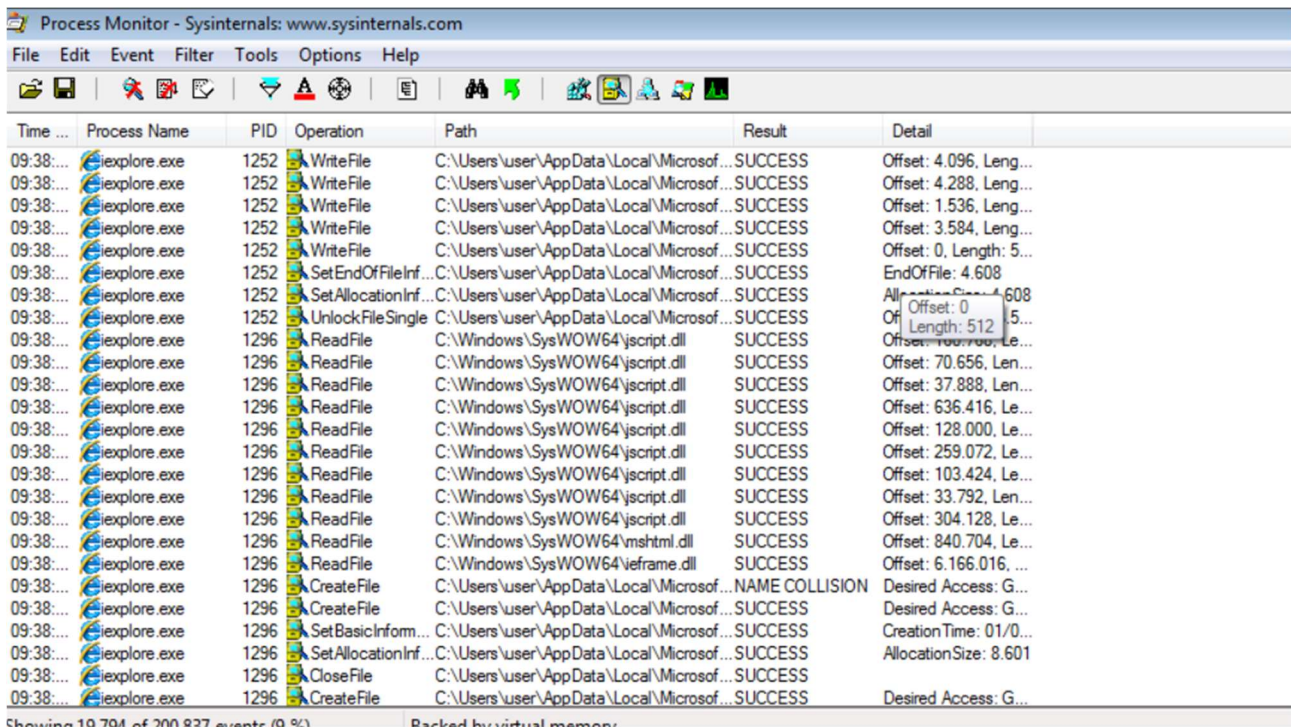


Traccia:

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.

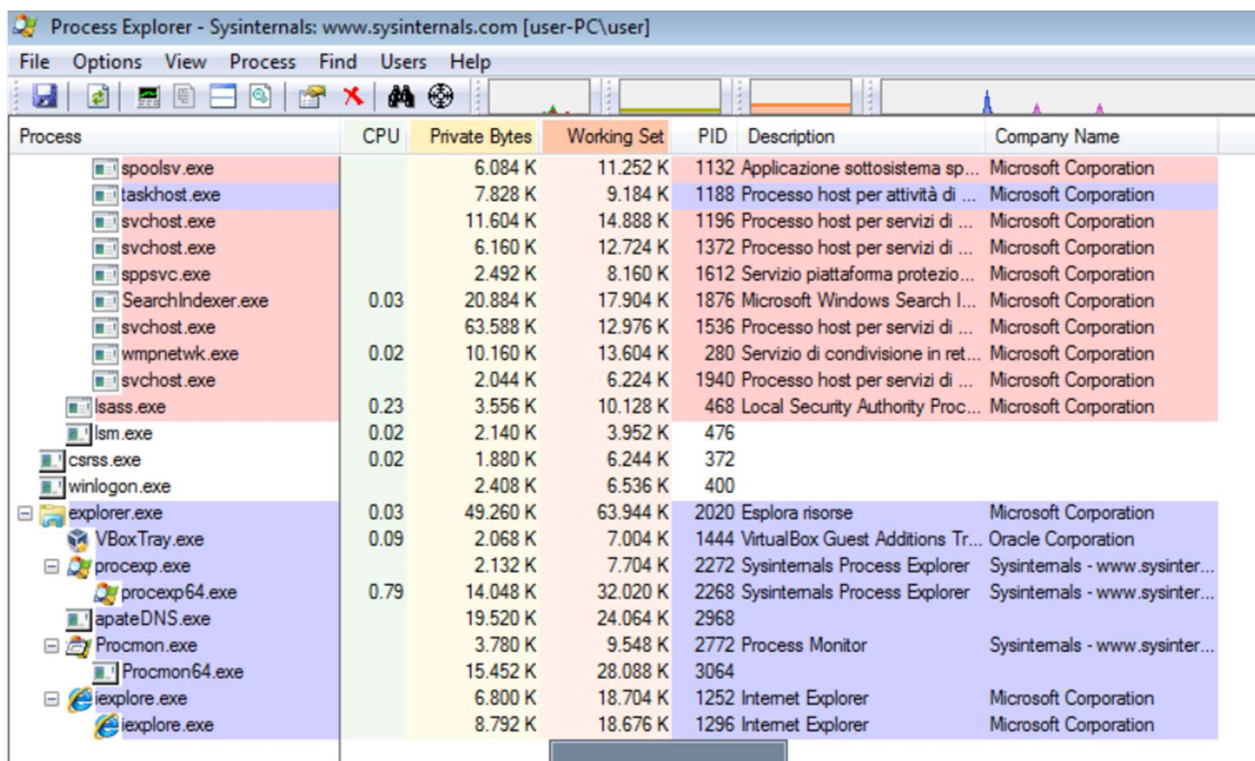


Process Monitor - Sysinternals: www.sysinternals.com

Time ...	Process Name	PID	Operation	Path	Result	Detail
09:38:...	iexplore.exe	1252	WriteFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 4.096, Leng...
09:38:...	iexplore.exe	1252	WriteFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 4.288, Leng...
09:38:...	iexplore.exe	1252	WriteFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 1.536, Leng...
09:38:...	iexplore.exe	1252	WriteFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 3.584, Leng...
09:38:...	iexplore.exe	1252	WriteFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 0, Length: 5...
09:38:...	iexplore.exe	1252	SetEndOfFileInf...	C:\Users\user\AppData\Local\Microsof...	SUCCESS	EndOfFile: 4.608
09:38:...	iexplore.exe	1252	SetAllocationInf...	C:\Users\user\AppData\Local\Microsof...	SUCCESS	AllocationSize: 8.601
09:38:...	iexplore.exe	1252	UnlockFileSingle	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Offset: 0, Length: 512
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 70.656, Len...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 37.888, Len...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 636.416, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 128.000, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 259.072, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 103.424, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 33.792, Len...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\jscript.dll	SUCCESS	Offset: 304.128, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\mshtml.dll	SUCCESS	Offset: 840.704, Le...
09:38:...	iexplore.exe	1296	ReadFile	C:\Windows\SysWOW64\eframe.dll	SUCCESS	Offset: 6.166.016, ...
09:38:...	iexplore.exe	1296	CreateFile	C:\Users\user\AppData\Local\Microsof...	NAME COLLISION	Desired Access: G...
09:38:...	iexplore.exe	1296	CreateFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Desired Access: G...
09:38:...	iexplore.exe	1296	SetBasicInform...	C:\Users\user\AppData\Local\Microsof...	SUCCESS	CreationTime: 01/0...
09:38:...	iexplore.exe	1296	SetAllocationInf...	C:\Users\user\AppData\Local\Microsof...	SUCCESS	AllocationSize: 8.601
09:38:...	iexplore.exe	1296	CloseFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	
09:38:...	iexplore.exe	1296	CreateFile	C:\Users\user\AppData\Local\Microsof...	SUCCESS	Desired Access: G...

Showing 10,704 of 200,827 events (0 %)

Paused by virtual memory



Process Explorer - Sysinternals: www.sysinternals.com [user-PC\user]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
spoolsv.exe		6.084 K	11.252 K	1132	Applicazione sottosistema sp...	Microsoft Corporation
taskhost.exe		7.828 K	9.184 K	1188	Processo host per attività di ...	Microsoft Corporation
svchost.exe		11.604 K	14.888 K	1196	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		6.160 K	12.724 K	1372	Processo host per servizi di ...	Microsoft Corporation
sppsvc.exe		2.492 K	8.160 K	1612	Servizio piattaforma protezio...	Microsoft Corporation
SearchIndexer.exe	0.03	20.884 K	17.904 K	1876	Microsoft Windows Search I...	Microsoft Corporation
svchost.exe		63.588 K	12.976 K	1536	Processo host per servizi di ...	Microsoft Corporation
wmpnetwk.exe	0.02	10.160 K	13.604 K	280	Servizio di condivisione in ret...	Microsoft Corporation
svchost.exe		2.044 K	6.224 K	1940	Processo host per servizi di ...	Microsoft Corporation
lsass.exe	0.23	3.556 K	10.128 K	468	Local Security Authority Proc...	Microsoft Corporation
lsim.exe	0.02	2.140 K	3.952 K	476		
csrss.exe	0.02	1.880 K	6.244 K	372		
winlogon.exe		2.408 K	6.536 K	400		
explorer.exe	0.03	49.260 K	63.944 K	2020	Esplora risorse	Microsoft Corporation
VBBoxTray.exe	0.09	2.068 K	7.004 K	1444	VirtualBox Guest Additions Tr...	Oracle Corporation
procexp.exe		2.132 K	7.704 K	2272	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	0.79	14.048 K	32.020 K	2268	Sysinternals Process Explorer	Sysinternals - www.sysinter...
apateDNS.exe		19.520 K	24.064 K	2968		
Procmon.exe		3.780 K	9.548 K	2772	Process Monitor	Sysinternals - www.sysinter...
Procmon64.exe		15.452 K	28.088 K	3064		
iexplore.exe		6.800 K	18.704 K	1252	Internet Explorer	Microsoft Corporation
iexplore.exe		8.792 K	18.676 K	1296	Internet Explorer	Microsoft Corporation

ieexplore.exe:1252 Properties

TCP/IP Security Environment Strings
Image Performance Performance Graph Threads

Count: 11

TID	CPU	Cycles Delta	Start Address
1036			ntdll.dll!RtlDosSearchPath_Ustr+0x69a
2572			ieexplore.exe+0x1c9a
2608			ntdll.dll!RtlLoadString+0x430
780			iertutil.dll!Ordinal59+0x53
1804			iertutil.dll!Ordinal536
1436			IEFRAME.dll!Ordinal317+0x7df
2784			rasman.dll!RasAddNotification+0x384
1648			WININET.dll!FindNextUrlCacheEntryEx...
2204			msvcrt.dll!_endthreadex+0x29
872			iertutil.dll!Ordinal405+0x1e
2100			ntdll.dll!RtlDosSearchPath_Ustr+0x69a

Thread ID: 2572 Stack Module

Start Time: 09:38:48 29/03/2024

State: Wait:WrUserRequest Base Priority: 8

Kernel Time: 0:00:00.671 Dynamic Priority: 12

User Time: 0:00:00.250 I/O Priority: Normal

Context Switches: 1.660 Memory Priority: 5

Cycles: 1.853.758.511 Ideal Processor: 0


```
w21d4 - Blocco note
File Modifica Formato Visualizza ?
Regshot 1.9.0 x64 ANSI
Comments:
Datetime: 2024/3/29 08:34:09 , 2024/3/29 08:39:38
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys deleted: 2
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum

-----
Keys added: 8
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell

-----
Values deleted: 6
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\services\PROCMON23\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\0: "Root\LEGACY_PROCMON23\0000"
HKLM\SYSTEM\CurrentControlSet\services\PROCMON23\Enum\Count: 0x00000001

-----
Values added: 13
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_PROCMON23\0000\Control\ActiveService: "PROCMON23"
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Internet Explorer\Recovery\Active\{C30E515D-EDA7-11EE-A62F-080027E
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3: 5C
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3\Nodes
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3\MRULi
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell\Knowr
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell\Sniff
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3: 5C 00 31 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3\NodeSlot: 0x00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\BagMRU\0\0\1\3\MRUListEX: FF
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell\KnownFolderDer
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\windows\shell\Bags\100\Shell\SniffedFolderI

-----
Values modified: 28
HKLM\SOFTWARE\Microsoft\windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000008
HKLM\SOFTWARE\Microsoft\windows\CurrentVersion\Explorer\GlobalAssocChangedCounter: 0x00000009
HKLM\SOFTWARE\Microsoft\windows\NT\CurrentVersion\PerFlib\CurrentLanguage\Counter: 31 00 31 38 34 37 00 32 00 53 69 73 74 65 6D 61 0C
2 69 61 20 76 69 6E 63 6F 6C 61 74 61 00 33 32 00 53 63 72 69 74 74 75 72 65 20 69 6E 20 63 6F 70 69 61 2F 73 65 63 00 33 34 00 45 72
67 69 6E 67 00 36 30 00 41 6C 6C 6F 63 61 7A 69 6F 6E 69 20 70 6F 6F 6C 20 64 69 20 70 61 67 69 6E 67 00 36 34 00 41 6C 6C 6F 63 61 7
69 74 74 75 72 65 20 6D 61 69 6C 73 6C 6F 74 2F 73 65 63 00 38 34 00 52 69 63 68 69 65 73 74 65 20 65 6C 65 6E 63 6F 20 73 65 72 76 65
4 75 72 61 20 74 72 6F 76 61 74 65 20 25 00 31 30 36 00 4C 65 74 74 75 72 65 20 69 6E 20 63 6F 70 69 61 2F 73 65 63 00 31 30 38 00 4C
74 75 72 65 20 76 65 6C 6F 63 69 20 61 73 69 6E 63 72 6F 6E 65 2F 73 65 63 00 31 33 30 00 4C 65 74 74 75 72 65 20 76 65 6C 6F 63 69 2
65 72 72 75 70 74 2F 73 65 63 00 31 35 30 00 43 68 69 61 6D 61 74 65 20 64 69 20 73 69 73 74 65 6D 61 2F 73 65 63 00 31 35 32 00 52 65
5 63 00 31 37 30 00 41 6C 6C 6F 63 61 7A 69 6F 6E 69 20 6D 61 69 6C 73 6C 6F 74 20 6E 6F 6E 20 72 69 75 73 63 69 74 65 00 31 37 32 00
```