

Progetto S10-Bonus

Studente: Simone Mininni

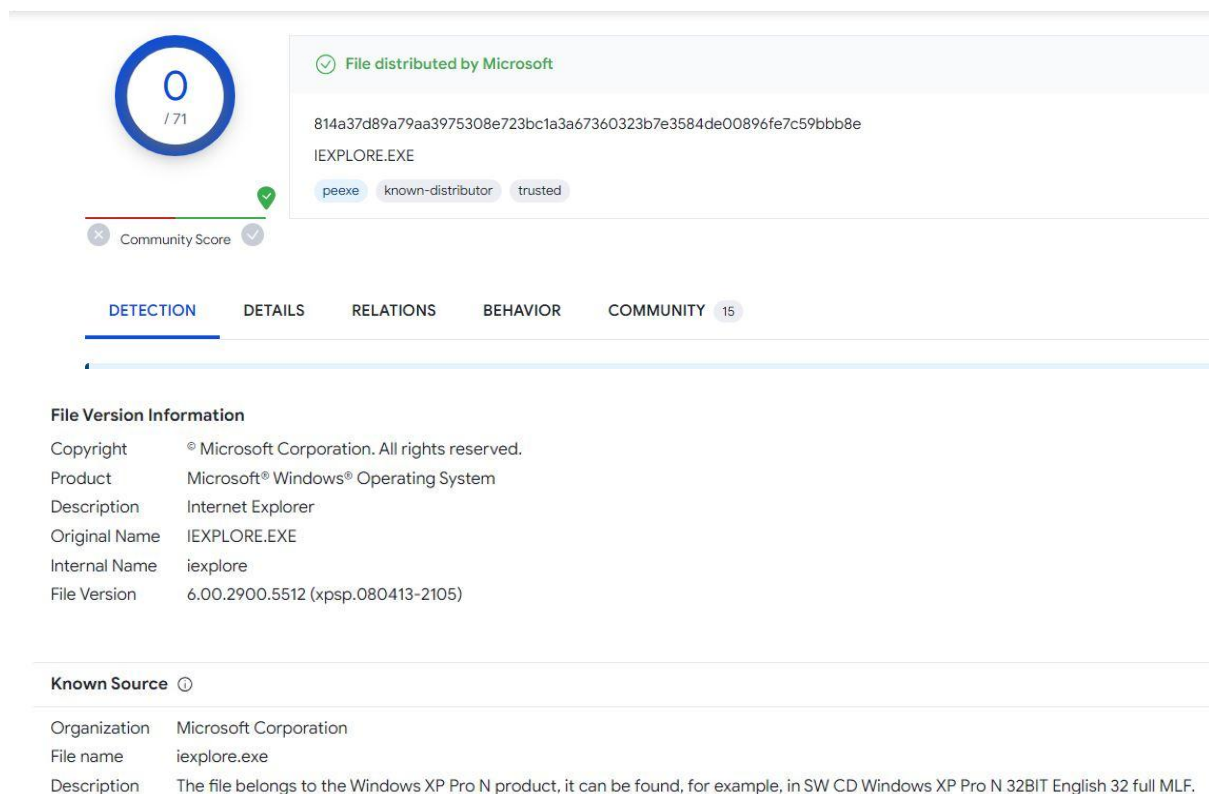
Task: Dimostrare che il file eseguibile IEXPLORE.EXE nella cartella C:\Program Files\Internet Explorer

Analisi Statica Base

Hash del file eseguibile:

- 55794B97A7FAABD2910873C85274F409 md5
- 814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e sha-256

Virus Total Analysis:



The screenshot shows the VirusTotal analysis interface for the file IEXPLORE.EXE. At the top, a large blue circle with the number '0' and '/71' indicates that no vendors have detected any threats. To the right, a green checkmark and the text 'File distributed by Microsoft' are displayed. Below this, the file's SHA-256 hash is shown: 814a37d89a79aa3975308e723bc1a3a67360323b7e3584de00896fe7c59bbb8e. The file name 'IEXPLORE.EXE' is listed, followed by three tags: 'peexe', 'known-distributor', and 'trusted'. A 'Community Score' section shows a green checkmark and a '15' in a circle. Below this, a tabbed interface with 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY' is shown, with 'DETECTION' selected. Under the 'DETECTION' tab, the 'File Version Information' section lists: Copyright © Microsoft Corporation. All rights reserved.; Product Microsoft® Windows® Operating System; Description Internet Explorer; Original Name IEXPLORE.EXE; Internal Name iexplore; and File Version 6.00.2900.5512 (xpsp.080413-2105). The 'Known Source' section shows: Organization Microsoft Corporation; File name iexplore.exe; and Description The file belongs to the Windows XP Pro N product, it can be found, for example, in SW CD Windows XP Pro N 32BIT English 32 full MLF.

71 vendor non hanno rilevato nessuna minaccia, e dalle informazioni più dettagliate possiamo notare che appartiene a Microsoft Corporation, ed è un programma di WinXp Pro.

Per il momento possiamo dire che non ci sono sospetti che si tratti di un malware.

PeStudio

Analisi delle strings:

x	-	<u>Signature</u>
x	-	<u>Browser Frame Start</u>
x	-	<u>GetCurrentThreadId</u>
x	-	<u>GetModuleFileName</u>
x	-	<u>UnmapViewOfFile</u>
x	-	<u>CreateProcess</u>
x	-	<u>GetCurrentProcessId</u>
x	-	<u>DuplicateHandle</u>
x	-	<u>MapViewOfFile</u>
x	-	<u>CreateFileMapping</u>
x	-	<u>GetModuleFileName</u>
x	-	<u>OpenProcess</u>
x	-	<u>TerminateProcess</u>
x	-	<u>GetForegroundWindow</u>
x	-	<u>GetShellWindow</u>
x	-	<u>PathFindFileName</u>
x	-	<u>PathRemoveFileSpec</u>

Possiamo vedere che sono state rilevate alcune funzioni di sistema sospette.

Librerie Importate:

SHDOCVW.dll

KERNEL32.dll

msvcrt.dll

SHLWAPI.dll

USER32.dll

File: test.exe									
Dos Header									
Nt Headers									
File Header									
Optional Header									
Data Directories [x]									
Section Headers [x]									
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00001D98	00001000	00001E00	00000400	00000000	00000000	0000	0000	60000020
.data	0000009C	00003000	00000200	00002200	00000000	00000000	0000	0000	C0000040
.rsrc	00014740	00004000	00014800	00002400	00000000	00000000	0000	0000	40000040

Le sezioni del programma sono tre, il programma è unpacked, quindi le sezioni sono visibili.

Analisi Dinamica Base

Evidenze durante l'esecuzione del codice:

Server Dns impostato sulla nostra macchina di laboratorio per catturare eventuali comunicazioni con la rete internet sospette.

Network signatures:

Wireshark:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	172.16.1.50	172.16.1.255	BROWSE	216	Get Backup List Request
2	0.00007600	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
3	0.74738300	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
4	1.49870300	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
5	4.24723700	172.16.1.50	172.16.1.255	BROWSE	216	Get Backup List Request
6	4.24738800	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
7	4.99717300	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
8	5.74784900	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
9	8.49785700	172.16.1.50	172.16.1.255	BROWSE	216	Get Backup List Request
10	8.49793800	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
11	9.24791600	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
12	9.99800500	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
13	12.74677200	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
14	13.49799200	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
15	14.24799200	172.16.1.50	172.16.1.255	NBNS	92	Name query NB WORKGROUP<1b>
16	52.27845400	172.16.1.50	172.16.1.255	BROWSE	243	Host Announcement MALWARE_TEST, workstation, Server, NT workstation

All'avvio del programma notiamo una comunicazione verso l'indirizzo di broadcast della nostra rete di laboratorio.

Quindi non ci sono request verso domini specifici o indirizzi ip pubblici.

Procmon:

Time of Day	Process Name	PID	Operation	Path
1:45:11.79586...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1089 -> Malware_test:8000
1:45:12.34372...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1089 -> Malware_test:8000
1:45:12.34385...	IEEXPLORE.EXE	632	TCP Disconnect	Malware_test:1089 -> Malware_test:8000
1:45:52.80952...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1090 -> Malware_test:8000
1:45:53.35972...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1090 -> Malware_test:8000
1:45:53.35988...	IEEXPLORE.EXE	632	TCP Disconnect	Malware_test:1090 -> Malware_test:8000
1:46:13.04805...	IEEXPLORE.EXE	3628	UDP Receive	localhost:1091 -> localhost:1091
1:46:13.04805...	IEEXPLORE.EXE	3628	UDP Send	localhost:1091 -> localhost:1091
1:46:13.59136...	IEEXPLORE.EXE	3628	TCP Reconnect	Malware_test:1092 -> Malware_test:http
1:46:14.13768...	IEEXPLORE.EXE	3628	TCP Reconnect	Malware_test:1092 -> Malware_test:http
1:46:14.13776...	IEEXPLORE.EXE	3628	TCP Disconnect	Malware_test:1092 -> Malware_test:http
1:46:33.82344...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1093 -> Malware_test:8000
1:46:34.37123...	IEEXPLORE.EXE	632	TCP Reconnect	Malware_test:1093 -> Malware_test:8000
1:46:34.37132...	IEEXPLORE.EXE	632	TCP Disconnect	Malware_test:1093 -> Malware_test:8000

Vediamo anche con procmon che le richieste vengono effettuate sempre verso la nostra macchina locale che fa da server dns, quindi nel programma non ci sono indicazioni per una connessione malevola verso uno specifico server dns o dominio.

Host signatures: Processi e thread

IEXPLORE.EXE	632	Thread Create	
IEXPLORE.EXE	632	Thread Exit	
IEXPLORE.EXE	632	Thread Create	
IEXPLORE.EXE	632	Thread Exit	
IEXPLORE.EXE	3628	Process Start	
IEXPLORE.EXE	3628	Thread Create	
IEXPLORE.EXE	3628	Load Image	C:\Documents and Settings\Administrator\Desktop\IEXPLORE.EXE
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\ntdll.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\kernel32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\user32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\gdi32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\shlwapi.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\advapi32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\RPCRT4.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\Secur32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\shdocvw.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\crypt32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\asn1.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\cryptui.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\metapi32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\oleaut32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\ole32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\version.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\wininet.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\wintrust.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\imagehlp.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\ldap32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\shimeng.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\riched20.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\shell32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\comctl32.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\uxtheme.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\browserui.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\browserid.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\apphelp.dll
IEXPLORE.EXE	3628	Load Image	C:\WINDOWS\system32\olecat.dll

Non sono rilevati creazioni di nuovi processi, solo thread come usualmente i browser fanno.

Comportamento nella norma.

Explorer.EXE (264)	Windows Explorer	C:\WINDOWS\E...		Microsoft Corporat...	MAL
VBBoxTray.exe (500)	VirtualBox Guest ...	C:\WINDOWS\sy...		Oracle Corporation	MAL
apateDNS.exe (2784)	Mandiant	C:\Documents an...		Mandiant	MAL
Procmon.exe (2780)	Process Monitor	C:\Documents an...		Sysinternals - ww...	MAL
IEXPLORE.EXE (3384)	Internet Explorer	C:\Documents an...		Microsoft Corporat...	MAL
cmd.exe (396)	Windows Comma...	C:\WINDOWS\sy...		Microsoft Corporat...	NT /

Dall' albero dei processi, notiamo che il file target non genera nessun processo figlio(shell ad esempio).

Anche dall'analisi del filesystem, non ci sono creazioni di file sospetti o eliminazioni.

Attività sui registri:

Regshot:

```
Regshot 1.9.0 x86 unicode
Comments:
Datetime: 2023/12/1 13:45:56 , 2023/12/1 13:46:20
Computer: MALWARE_TEST , MALWARE_TEST
Username: Administrator , Administrator

-----
values modified: 11
HKLM\SOFTWARE\Microsoft\Cryptography\ RNGSeed: CC 04 B3 38 69 EB 3C BF B3 19 60 14 E1 19 7A 48 83 E8 61 13 0F 80 21 80 AF 7F 19 20 E5 A7 2A 90 CE 01 ED F1 13 08 13 1C DC 12 13 72 71 F6 B7
HKLM\SOFTWARE\Microsoft\Cryptography\ RNGSeed: 33 0F 4D 65 F3 85 7C 37 48 E9 FC 19 56 08 66 8B 60 CE 4D E9 44 43 00 98 97 0B E2 A2 65 87 99 F9 80 F1 CB B0 F1 25 00 32 BE 0C 02 40 BA 0A B1
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_LHACNGU: 0F 00 00 00 03 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_LHACNGU: 0F 00 00 00 04 01
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_HVFPHG: 0F 00 00 00 19 01 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_HVFPHG: 0F 00 00 00 1A 01 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_LHACNGU:P:\qbphzragf naq Ffg
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\VRZR_LHACNGU:P:\qbphzragf naq Ffg
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Count: 0x00000005
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Count: 0x00000006
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Time: E7 07 0C 00 05 00 01 00 00 00 28
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Time: E7 07 0C 00 05 00 01 00 00 00 2E
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Time: E7 07 0C 00 05 00 01 00 00 00 2E
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F85F1910-F110-1102-BB9E-00C04F795683}\Explorer\Count: 0x00000005
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F85F1910-F110-1102-BB9E-00C04F795683}\Explorer\Count: 0x00000006
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F85F1910-F110-1102-BB9E-00C04F795683}\Explorer\Time: E7 07 0C 00 05 00 01 00 00 00 28
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{F85F1910-F110-1102-BB9E-00C04F795683}\Explorer\Time: E7 07 0C 00 05 00 01 00 00 00 2E
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 39 00 00 00 01 00 00 00 00 00 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 39 00 00 00 01 00 00 00 00 00 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\Shell\NORAM\BagMRU\VRULstEx: 02 00 00 00 06 00 00 00 0A 00 00 00 07 00 00 00 00 17 00 00 00 02 00 00 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\Software\Microsoft\Windows\Shell\NORAM\BagMRU\VRULstEx: 02 00 00 00 02 00 00 00 06 00 00 00 0A 00 00 00 07 00 00 00 17 00 00 00 02 00 00 0
HKU\S-1-5-21-1993962763-1606980848-725345543-500\SessionInformation\ProgramCount: 0x00000003
HKU\S-1-5-21-1993962763-1606980848-725345543-500\SessionInformation\ProgramCount: 0x00000004

-----
Total changes: 111
-----
```

Procmon:

Confronto con regshot rispetto ai registri modificati dal file eseguibile in esame:

	IEXPLORE.EXE	3628		RegQueryValue	HKCU\Software\Microsoft\Windows\Shell\NoRoam\BagMRU\VRULstEx	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegSetValue	HKCU\Software\Microsoft\Windows\Shell\NoRoam\BagMRU\VRULstEx	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegQueryValue	HKCU\Software\Microsoft\Windows\Shell\NoRoam\BagMRU\VRULstEx	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegSetValue	HKCU\Software\Microsoft\Windows\Shell\NoRoam\BagMRU\VRULstEx	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Count	SUCCESS	Type: REG_DWORD
	IEXPLORE.EXE	3628		RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{E2E20038-0088-4134-82B7-F2BA38496583}\Explorer\Count	SUCCESS	Type: REG_DWORD
	IEXPLORE.EXE	3628		RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegQueryValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_BINARY,
	IEXPLORE.EXE	3628		RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS	Type: REG_BINARY,

Interventi ordinari del browser di windows.

Si vanno a modificare solo le chiavi di registro dello user corrente.

Nessuna attività sospetta.

In conclusione dall' analisi Statica e dinamica base, non sono riuscito a rilevare evidenze che IEXPLORE.EXE sia un malware.

Fine.