



# S10/L5

---

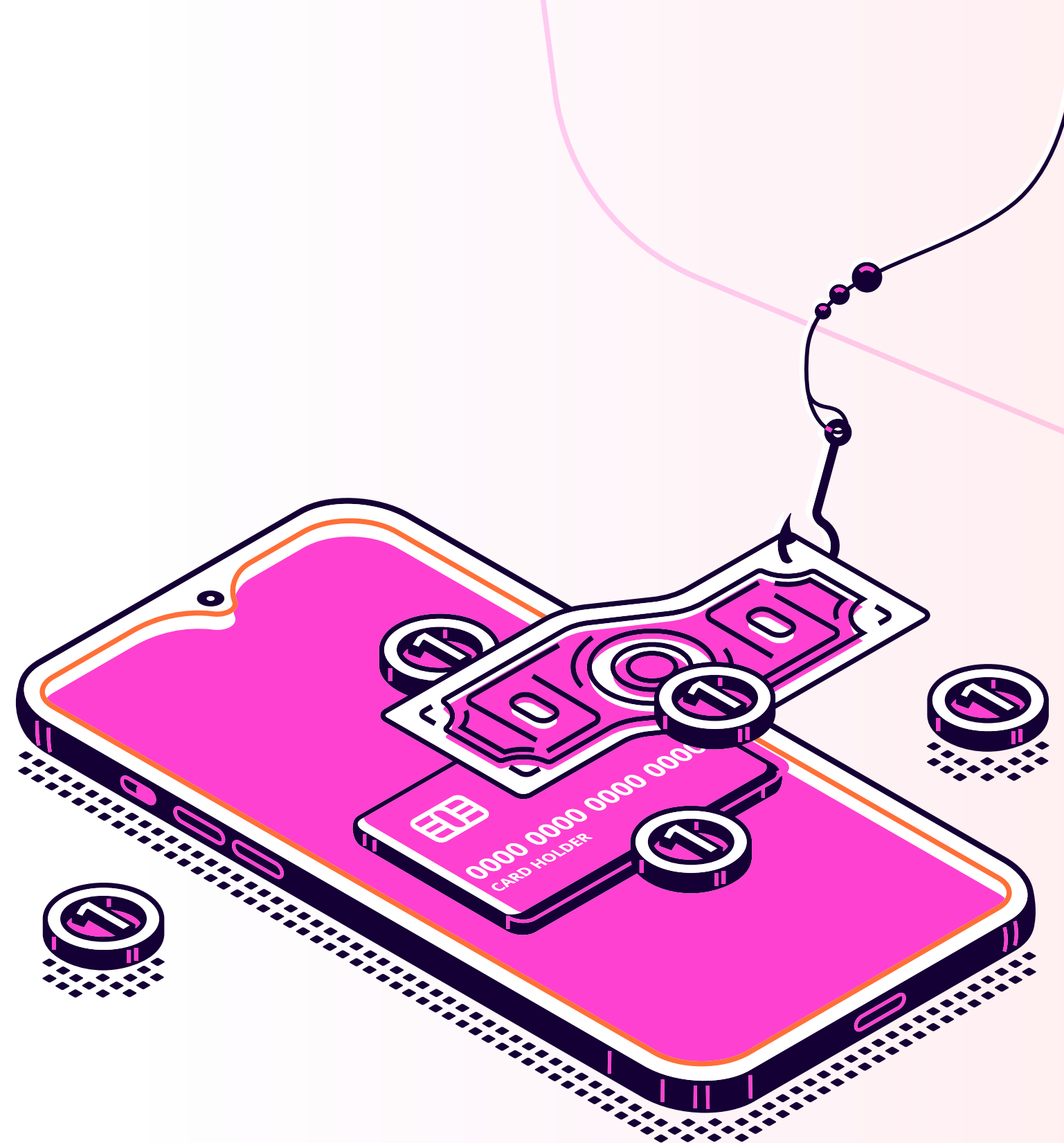
BONUS

# 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.

Possono essere usati gli strumenti di analisi statica basica e/o analisi dinamica basica visti a lezione. **No disassembly no debug o simili VirusTotal non basta, ovviamente Non basta dire iexplorer è Microsoft quindi è buono, punto.**



# ANALISI STATICA

Per risolvere questo problema e convincere il carissimo giovane dipendente che il file "iexplore.exe" non è maligno, effettuerò una serie di analisi basiche statiche e dinamiche. Inizierò col verificare il suddetto file nella sua canonica directory:

**C:\Programmi\Internet Explorer\iexplore.exe**. Dopodichè, tramite **certutil** integrato in windows (questa volta non utilizzerò md5deep), verificherò l'hash **SHA1** dell'eseguibile.

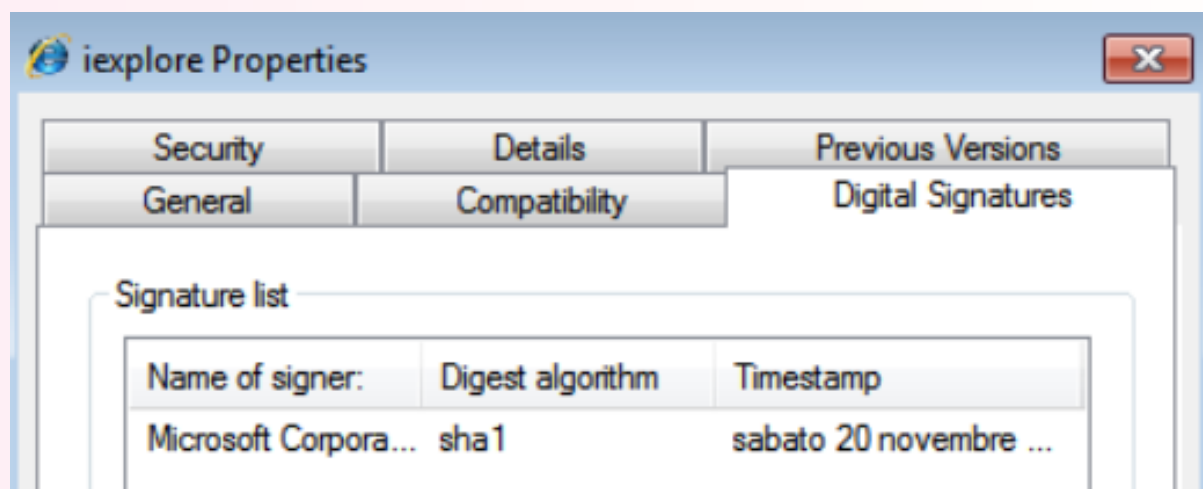
```
C:\Users\Admin\Desktop
λ certutil -hashfile "C:\Program Files\Internet Explorer\iexplore.exe"
SHA1 hash of file C:\Program Files\Internet Explorer\iexplore.exe:
2a a8 59 f0 08 fa fb ae fb 57 80 19 ed 0d 65 cd 09 33 98 1c
CertUtil: -hashfile command completed successfully.
```

Poi, con un tool integrato in sysinternal chiamato sigcheck, verificò la firma digitale, dimostrando che è stato firmato da nientepopodimeno che **Microsoft** in persona.

```
C:\Users\Admin\Desktop\Software Malware analysis\SysinternalsSuite
λ sigcheck.exe -i "C:\Program Files\Internet Explorer\iexplore.exe"

Sigcheck v2.1 - File version and signature viewer
Copyright (C) 2004-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\program files\internet explorer\iexplore.exe:
  Verified: Signed
  Catalog: C:\Windows\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\Microsoft-Windows-InternetExp
  lorer-Optional-Package~31bf3856ad364e35~amd64~~8.0.7601.17514.cat
  Signers:
    Microsoft Windows
      Status: A required certificate is not within its validity period when verifying against the current sy
      stem clock or the timestamp in the signed file.
      Valid Usage: Code Signing, NT5 Crypto
      Serial Number: 61 15 23 0F 00 00 00 00 00 0A
      Thumbprint: 02ECEEA9D5E0A9F3E39B6F4EC3F7131ED04E352C4
      Algorithm: SHA1
      Valid from: 23:57 07/12/2009
      Valid to: 23:57 07/03/2011
    Microsoft Windows Verification PCA
      Status: A required certificate is not within its validity period when verifying against the current sy
      stem clock or the timestamp in the signed file.
      Valid Usage: Code Signing, NT5 Crypto
      Serial Number: 61 07 02 DC 00 00 00 00 00 0B
      Thumbprint: 5DF0D7571B0780783960C68B78571FFD7EDAF021
      Algorithm: SHA1
      Valid from: 23:55 15/09/2005
      Valid to: 00:05 16/03/2016
    Microsoft Root Certificate Authority
      Status: A required certificate is not within its validity period when verifying against the current sy
      stem clock or the timestamp in the signed file.
      Valid Usage: All
      Serial Number: 79 AD 16 A1 4A A0 A5 AD 4C 73
      Thumbprint: 58 F4 07 13 2E 65
      Algorithm: SHA1
      Valid from: 01:19 10/05/2001
      Valid to: 01:28 10/05/2021
```





# ANALISI STATICA

La verifica delle firme digitali e delle proprietà dei file è cruciale per garantire l'integrità e l'autenticità del software. Non ci siamo limitati a dire semplicemente: "Internet Explorer è di Microsoft, quindi è sicuro." **Abbiamo effettuato controlli specifici per confermare che il file sia effettivamente firmato da Microsoft.** Questo processo include l'esame della firma digitale per assicurarsi che non sia stata alterata e che provenga dalla fonte dichiarata, dimostrando così che il file non è stato compromesso o manomesso. Passiamo ora a strings. Da come si vede, parecchie stringhe all'interno dell'exe fanno riferimento a microsoft e i suoi domini internet.

```
cmd
Microsoft Code Signing PCA
1D0B
"Microsoft Window
http://www.microsoft.com0
)T>
35W
s$[v/
t*K
n$<{
m`M]S
gDg
cNb
>~/
0w1
US1
Washington1
Redmond1
Microsoft Corporation1!0
Microsoft Time-Stamp PCA
101120132825Z0#
d0#
>C$
8z@<RN
n^(9
S0)
#L0
=>gC

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
ProductVersion
8.00.7601.17514
0c0904E4
CompanyName
Microsoft Corporation
FileDescription
Internet Explorer
FileVersion
8.00.7601.17514
InternalName
iexplore
LegalCopyright
Microsoft Corporation. All rights reserved.
OriginalFilename
IEXPLORE.EXE

Microsoft Corporation1#0!
Microsoft Code Signing PCA0

8http://crl.microsoft.com/pki/crl/products/CodeSigPCA.crl0M
A0?0=
1http://www.microsoft.com/pki/certs/CodeSigPCA.crt0
A]=\+
```

# ANALISI STATICA

Proviamo a controllare l'eseguibile anche su **CFF Explorer**. E' un browser, quindi è normale che faccia utilizzo massiccio di determinate funzioni. Le sezioni non sono oscurate, caso molto difficile per un malware che solitamente tenta di nascondere le sezioni.

File: iexplore.exe

Dos Header

Nt Headers

File Header

Optional Header

Data Directories [x]

Section Headers [x]

Import Directory

Resource Directory

Exception Directory

Relocation Directory

Debug Directory

Address Converter

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbe
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.text	00007349	00001000	00007400	00000400	00000000	00000000	0000	0000
.rdata	00007C08	00009000	00007E00	00007800	00000000	00000000	0000	0000
.data	00000B0C	00011000	00000A00	0000F600	00000000	00000000	0000	0000
.pdata	00000564	00012000						0000
.rsrc	00097020	00013000						0000
.reloc	00000674	000AB000						0000

iexplore.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderCh
szAnsi	(nFunctions)	Dword	Dword	Dword
ADVAPI32.dll	13	0000F6B8	FFFFFFFF	FFFFFFFF
KERNEL32.dll	56	0000F728	FFFFFFFF	FFFFFFFF
USER32.dll	9	0000F8F0	FFFFFFFF	FFFFFFFF
msvcrt.dll	29	0000F940	FFFFFFFF	FFFFFFFF
ntdll.dll	3	0000FA30	FFFFFFFF	FFFFFFFF
SHLWAPI.dll	23	0000FA50	FFFFFFFF	FFFFFFFF
SHELL32.dll	7	0000FB10	FFFFFFFF	FFFFFFFF
ole32.dll	5	0000FB50	FFFFFFFF	FFFFFFFF
iertutil.dll	14	0000FB80	FFFFFFFF	FFFFFFFF
urlmon.dll	3	0000FBF8	FFFFFFFF	FFFFFFFF

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 DINAMICA

Utilizziamo adesso **apataDNS** per fare da proxy e carpire le richieste di **iexplore.exe**, e Wireshark per intercettare e analizzare il traffico di rete.

The screenshot displays three overlapping windows illustrating network traffic analysis:

- Google - Windows Internet Explorer:** Shows the Google homepage with the URL `https://www.google.com/?gws_rd=ssl`.
- ApatDNS:** A proxy application window showing a list of domains requested. The list includes:

Time	Domain Requested
16:12:06	teredo.ipv6.microsoft.com
16:12:13	go.microsoft.com
16:12:13	go.microsoft.com
16:12:15	ieonline.microsoft.com
16:12:15	ieonline.microsoft.com
16:13:11	o.pki.goog
16:13:11	o.pki.goog
16:13:16	c.pki.goog
16:13:16	c.pki.goog
16:13:21	www.google.com
16:13:21	www.google.com
- Cattura da Local Area Connection (Wireshark):** A network traffic capture window showing a list of packets. The list includes:

No.	Time	Source	Destination	Protocol	Length	Info
338	58.476965	20.191.45.158	192.168.67.2	TCP	66	443 → 49226 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SA...
339	58.477302	192.168.67.2	20.191.45.158	TCP	54	49226 → 443 [ACK] Seq=1 Ack=1 Win=66240 Len=0
340	58.480354	192.168.67.2	20.191.45.158	TLSv1	188	Client Hello
341	58.536262	20.191.45.158	192.168.67.2	TCP	60	443 → 49226 [ACK] Seq=1 Ack=135 Win=64512 Len=0
342	58.536635	20.191.45.158	192.168.67.2	TLSv1	61	Alert (Level: Fatal, Description: Protocol Version)
343	58.536909	20.191.45.158	192.168.67.2	TCP	60	443 → 49226 [FIN, ACK] Seq=8 Ack=135 Win=64512 Len=0
344	58.537156	192.168.67.2	20.191.45.158	TCP	54	49226 → 443 [ACK] Seq=135 Ack=9 Win=66232 Len=0
345	58.539173	192.168.67.2	20.191.45.158	TCP	54	49226 → 443 [FIN, ACK] Seq=135 Ack=9 Win=66232 Len=0
346	58.540910	192.168.67.2	20.191.45.158	TCP	66	49227 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
347	58.594808	20.191.45.158	192.168.67.2	TCP	60	443 → 49226 [ACK] Seq=9 Ack=136 Win=64512 Len=0
348	58.598756	20.191.45.158	192.168.67.2	TCP	66	443 → 49227 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1440 SA...
349	58.599046	192.168.67.2	20.191.45.158	TCP	54	49227 → 443 [ACK] Seq=1 Ack=1 Win=66240 Len=0
350	58.601872	192.168.67.2	20.191.45.158	TLSv1	188	Client Hello
351	58.656177	20.191.45.158	192.168.67.2	TCP	60	443 → 49227 [ACK] Seq=1 Ack=135 Win=64512 Len=0
352	58.656496	20.191.45.158	192.168.67.2	TLSv1	61	Alert (Level: Fatal, Description: Protocol Version)
353	58.656722	20.191.45.158	192.168.67.2	TCP	60	443 → 49227 [FIN, ACK] Seq=8 Ack=135 Win=64512 Len=0

Anche in questo caso nessuna richiesta strana, solo i domini di microsoft e di google (che ho richiesto io visitando google.com da internet explorer).

# ANALISI DINAMICA

Nel caso di Wireshark **nessun indirizzo IP strano**. A parte tanta, tantissima **telemetria** (disattivabile attraverso degli script), gli ip analizzati fanno parte di **Microsoft** e di **Google**, nessuna richiesta sospetta. Solo tanto rumore.

ea Connection		
Analizza Vai Cattura Analizza Statistiche Telefoni		
Analizzazione ... <Ctrl-/>		
Source	Destination	
20.191.45.158	192.168.67.2	
192.168.67.2	20.191.45.158	
192.168.67.2	20.191.45.158	
20.191.45.158	192.168.67.2	
20.191.45.158	192.168.67.2	
20.191.45.158	192.168.67.2	
192.168.67.2	20.191.45.158	
192.168.67.2	20.191.45.158	
192.168.67.2	20.191.45.158	
20.191.45.158	192.168.67.2	
20.191.45.158	192.168.67.2	
192.168.67.2	20.191.45.158	
192.168.67.2	20.191.45.158	
20.191.45.158	192.168.67.2	
20.191.45.158	192.168.67.2	

```
flavio@MacBook-Pro ~ % whois 20.191.45.158
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer:      whois.arin.net

inetnum:    20.0.0.0 - 20.255.255.255
organisation: Administered by ARIN
status:     LEGACY

whois:      whois.arin.net

changed:    1994-10
source:     IANA

# whois.arin.net

NetRange:   20.180.0.0 - 20.191.255.255
CIDR:       20.184.0.0/13, 20.180.0.0/14
NetName:    MSFT
NetHandle:  NET-20-180-0-0-1
Parent:     NET20 (NET-20-0-0-0-0)
NetType:    Direct Allocation
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate:    2017-02-22
Updated:    2017-02-22
```

```
flavio@MacBook-Pro ~ % dig 20.191.45.158 MX
; <<>> DiG 9.10.6 <<>> 20.191.45.158 MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NXDOMAIN, id: 17791
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;20.191.45.158.                IN      MX

;; AUTHORITY SECTION:
.                43085   IN      SOA      a.root-servers.net. nstld.verisign-grs.com.
.                2024080200 1800 900 604800 86400

;; Query time: 61 msec
;; SERVER: 192.168.1.7#53(192.168.1.7)
;; WHEN: Fri Aug 02 16:24:19 CEST 2024
;; MSG SIZE rcvd: 117
```

```
flavio@MacBook-Pro ~ % curl -I 20.191.45.158
HTTP/1.1 301 Moved Permanently
Server: Microsoft-Azure-Application-Gateway/v2
Date: Fri, 02 Aug 2024 14:24:55 GMT
Content-Type: text/html
Content-Length: 195
Connection: keep-alive
Location: https://20.191.45.158/
```



# ANALISI DINAMICA

Per ulteriore conferma, possiamo utilizzare ProcMon per osservare l'attività del file. Se analizziamo il comportamento di "iexplore.exe" con ProcMon, vedremo che si comporta come previsto per un'applicazione legittima, **senza attività sospette**.

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time ...	Process Name	PID	Operation	Path	Result Detail
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS Desired Access: Query Value, Enumerate Sub Keys
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Length: 1,024
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Read
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS Desired Access: Read
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 1,024
16:22...	iexplore.exe	2416	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND Desired Access: Query Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS Desired Access: Query Value, Enumerate Sub Keys
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS KeySetInformationClass: KeySetHandle TagsInformation, Length: 0
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Length: 1,024
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Read
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS Desired Access: Read
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 1,024
16:22...	iexplore.exe	2416	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Query Value, Set Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desired Access: Query Value, Set Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Read
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Desired Access: Read
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\Software\Wow6432Node\Polici...	REPARSE Desired Access: Query Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS Desired Access: Query Value
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS KeySetInformationClass: KeySetHandle TagsInformation, Length: 0
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND Length: 80
16:22...	iexplore.exe	2416	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\...	SUCCESS
16:22...	iexplore.exe	2416	RegOpenKey	HKCU\Software\Policies\Microsoft\Win...	NAME NOT FOUND Desired Access: Query Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Read
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS Desired Access: Read
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS KeySetInformationClass: KeySetHandle TagsInformation, Length: 0
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS Type: REG_SZ, Length: 36, Data: 00060101.00060101
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 260
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS Type: REG_SZ, Length: 36, Data: 00060101.00060101
16:22...	iexplore.exe	2416	RegOpenKey	HKLM	SUCCESS Desired Access: Maximum Allowed, Granted Access: Read
16:22...	iexplore.exe	2416	RegQueryValue	HKLM	SUCCESS Query: Handle Tags, Handle Tags: 0x0
16:22...	iexplore.exe	2416	RegQueryValue	HKLM	SUCCESS Query: Name
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	NAME NOT FOUND Desired Access: Read
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE Desired Access: Query Value
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS Desired Access: Read
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS KeySetInformationClass: KeySetHandle TagsInformation, Length: 0
16:22...	iexplore.exe	2416	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 16
16:22...	iexplore.exe	2416	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS Desired Access: Read
16:22...	iexplore.exe	2416	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS KeySetInformationClass: KeySetHandle TagsInformation, Length: 0

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time ...	Process Name	PID	Operation	Path	Result Detail
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\Prefetch\IEXPLORE.EXE-	NAME NOT FOUND Desired Access: Generic Read, Disposition: Open, Options: S
16:22...	iexplore.exe	2416	CreateFile	C:\Windows	SUCCESS Desired Access: Execute/Traverse, Synchronize, Disposition:
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS Desired Access: Read Attributes, Disposition: Open, Options:
16:22...	iexplore.exe	2416	QueryBasicInfo	C:\Windows\System32\wow64.dll	SUCCESS CreationTime: 30/07/2024 11:50:02, LastAccessTime: 30/07
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS Desired Access: Read Data/List Directory, Execute/Traverse
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64.dll	FILE LOCKED WI... SyncType: SyncTypeCreateSection, PageProtection:
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64.dll	SUCCESS SyncType: SyncTypeOther
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS Desired Access: Read Attributes, Disposition: Open, Options:
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS CreationTime: 30/07/2024 11:49:54, LastAccessTime: 30/07
16:22...	iexplore.exe	2416	QueryBasicInfo	C:\Windows\System32\wow64win.dll	SUCCESS
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS Desired Access: Read Data/List Directory, Execute/Traverse
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI... SyncType: SyncTypeCreateSection, PageProtection:
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64cpu.dll	SUCCESS SyncType: SyncTypeOther
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS
16:22...	iexplore.exe	2416	QueryBasicInfo	C:\Windows\System32\wow64cpu.dll	SUCCESS Desired Access: Read Attributes, Disposition: Open, Options:
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS CreationTime: 30/07/2024 11:50:02, LastAccessTime: 30/07
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI... SyncType: SyncTypeCreateSection, PageProtection:
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\System32\wow64cpu.dll	SUCCESS SyncType: SyncTypeOther
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND Desired Access: Read Attributes, Disposition: Open, Options:
16:22...	iexplore.exe	2416	CreateFile	C:\Windows	SUCCESS Desired Access: Read Attributes, Synchronize, Disposition: O
16:22...	iexplore.exe	2416	QueryNameInfo	C:\Windows	SUCCESS Name: \Windows
16:22...	iexplore.exe	2416	CloseFile	C:\Windows	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Users\Admin	SUCCESS Desired Access: Execute/Traverse, Synchronize, Disposition:
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\SysWOW64\iehost.dll	SUCCESS Desired Access: Read Attributes, Disposition: Open, Options:
16:22...	iexplore.exe	2416	QueryBasicInfo	C:\Windows\SysWOW64\iehost.dll	SUCCESS CreationTime: 14/07/2009 01:11:59, LastAccessTime: 14/07
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\SysWOW64\iehost.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFile	C:\Windows\SysWOW64\iehost.dll	SUCCESS
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\SysWOW64\iehost.dll	FILE LOCKED WI... SyncType: SyncTypeCreateSection, PageProtection:
16:22...	iexplore.exe	2416	CreateFileMap	C:\Windows\SysWOW64\iehost.dll	SUCCESS SyncType: SyncTypeOther
16:22...	iexplore.exe	2416	CloseFile	C:\Windows\SysWOW64\iehost.dll	SUCCESS

Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
Time ...	Process Name	PID	Operation	Path	Result Detail
16:22...	iexplore.exe	3348	UDP Send	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Receive	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Connect	Admin-PC-49231 -> a92-123-114-109.de...	SUCCESS Length: 0, mss: 1460, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 65700, rcvwin...
16:22...	iexplore.exe	3348	UDP Send	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Receive	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Send	Admin-PC-49231 -> a92-123-114-109.de...	SUCCESS Length: 334, starttime: 242005, endtime: 242005, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Receive	Admin-PC-49231 -> a92-123-114-109.de...	SUCCESS Length: 376, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Send	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Receive	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Connect	Admin-PC-49232 -> a-0003.a-msedge.ne...	SUCCESS Length: 0, mss: 1440, sackopt: 1, tsopt: 0, wsopt: 1, rcvwin: 66240, rcvwin...
16:22...	iexplore.exe	3348	UDP Send	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Receive	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Send	Admin-PC-49232 -> a-0003.a-msedge.ne...	SUCCESS Length: 128, starttime: 242011, endtime: 242011, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	TCP Disconnect	Admin-PC-49232 -> a-0003.a-msedge.ne...	SUCCESS Length: 0, seqnum: 0, connid: 0
16:22...	iexplore.exe	3348	UDP Send	Admin-PC-56035 -> Admin-PC-56035	SUCCESS Length: 1, seqnum: 0, connid: 0



# Considerazioni finali

Caro Dipendente, abbiamo esaminato il file "**iexplore.exe**" che ci hai segnalato. Ecco i passaggi che abbiamo seguito per confermare che non è maligno: 1. Abbiamo verificato che il file si trova nella posizione legittima: "C:\Programmi\Internet Explorer". 2. Abbiamo controllato l'hash SHA-256 e la firma digitale del file, confermando che **è firmato** da "Microsoft Corporation". 3. Abbiamo eseguito il file in un ambiente controllato e **monitorato tutte le sue attività** con strumenti come **Procmon** e **Process Explorer**. Non sono state rilevate attività sospette. 4. Abbiamo monitorato il **traffico di rete** generato dal file e non abbiamo riscontrato comunicazioni anomale. Questi risultati ci portano a concludere che il file **è autentico e sicuro**. Grazie per la tua segnalazione e per la tua attenzione alla sicurezza.

PS: **Passa a Firefox!**





# **GRAZIE**

**Flavio Scognamiglio**