S10/L5

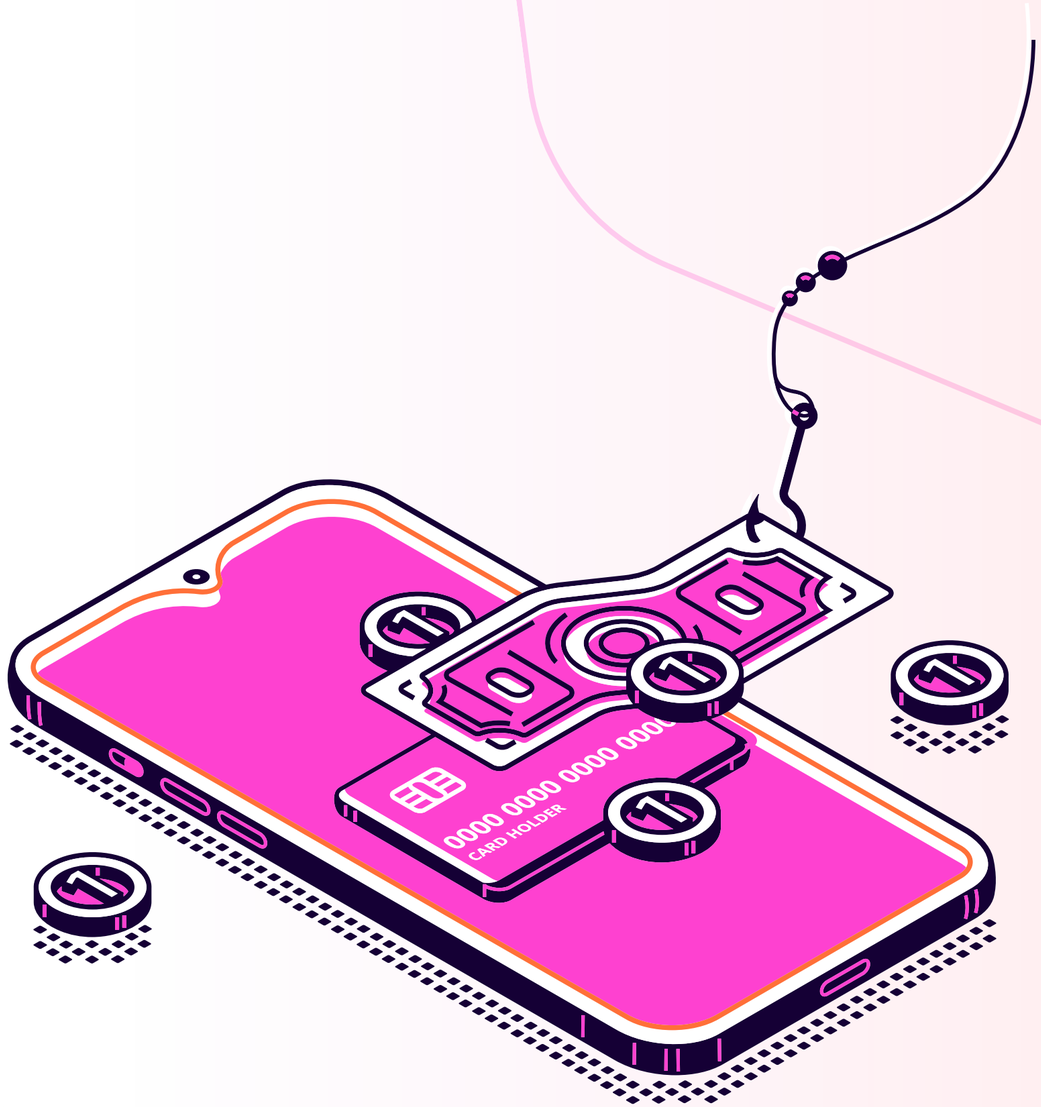
BONUS

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 similari VirusTotal non basta, ovviamente Non basta dire iexplorer è Microsoft quindi è buono, punto**.

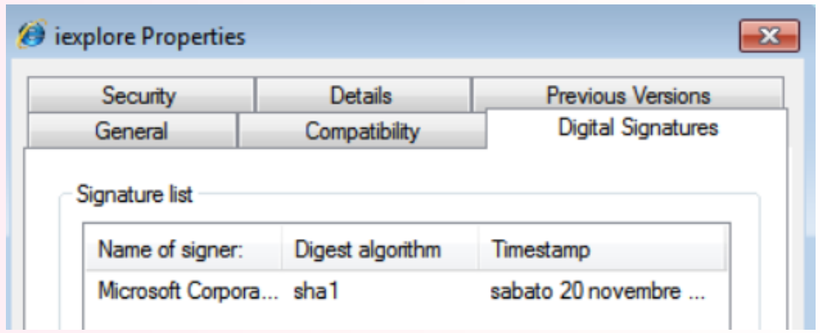


ANALISI STATICA

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.
```

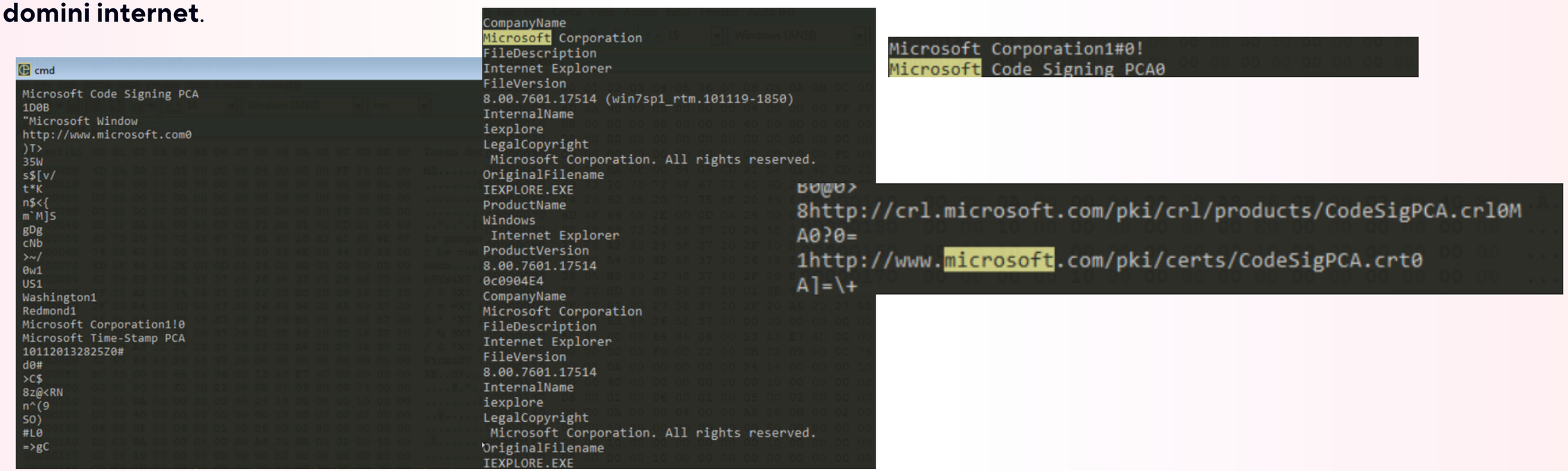
Poi, con un tool integrato in sysinternal chiamato sigcheck, verificò la firma digitale, dimostrando che è stato firmato da nientepopodimeno che **Microsoft** in persona.




```
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:     02ECEEA9D5E0A9F3E39B6F4EC3F7131ED4E352C4
                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
                                58 F4 07 13 2E 65
                Thumbprint:     CDD4EEAE6000AC7F40C3802C171E30148030C072
                Algorithm:      SHA1
                Valid from:     01:19 10/05/2001
                Valid to:       01:28 10/05/2021
```

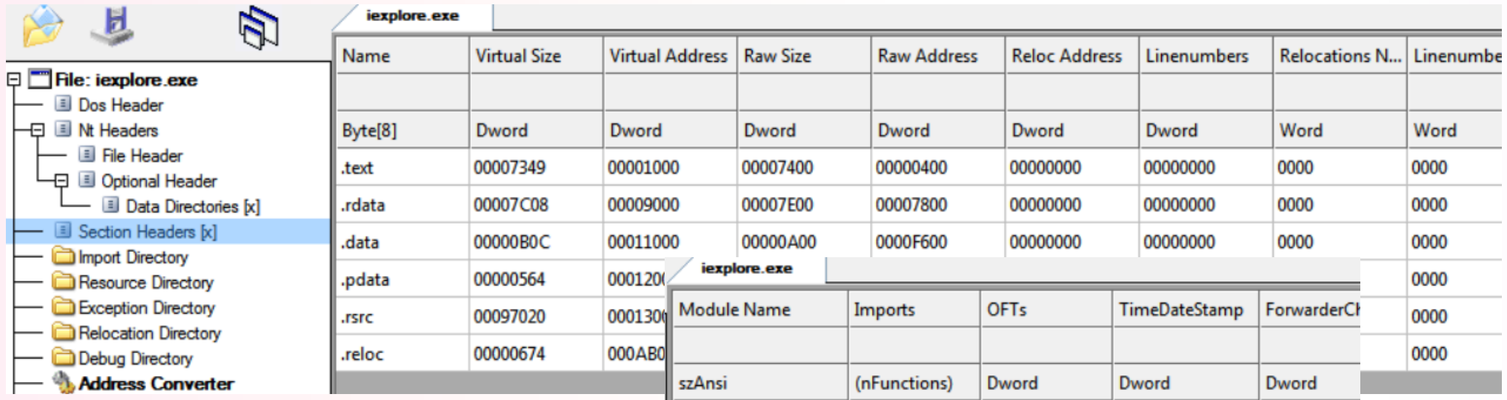
ANALISI STATICA

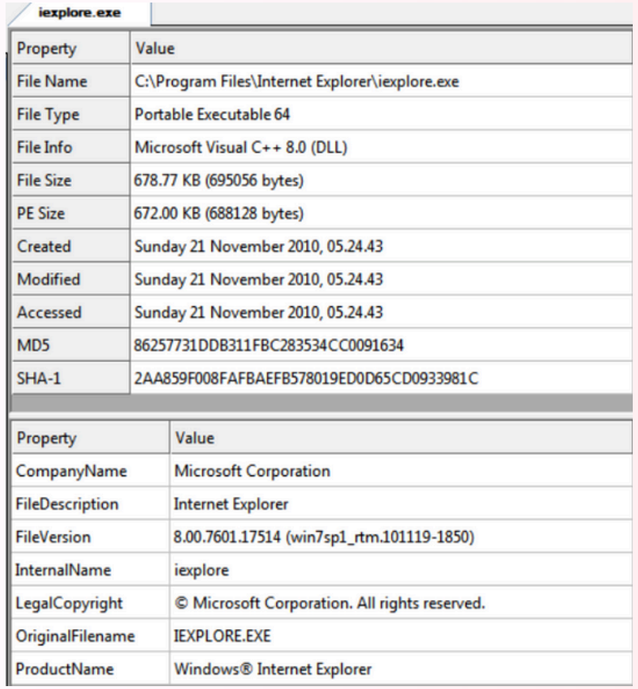
La verifica delle firme digitali e delle proprietà dei file è cruciale per garantire l'integrità e l'autenticità del software. Non ci siamo limitati a dire semplicemente: “Internet Explorer è di Microsoft, quindi è sicuro.” **Abbiamo effettuato controlli specifici per confermare che il file sia effettivamente 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**.



ANALISI STATICA

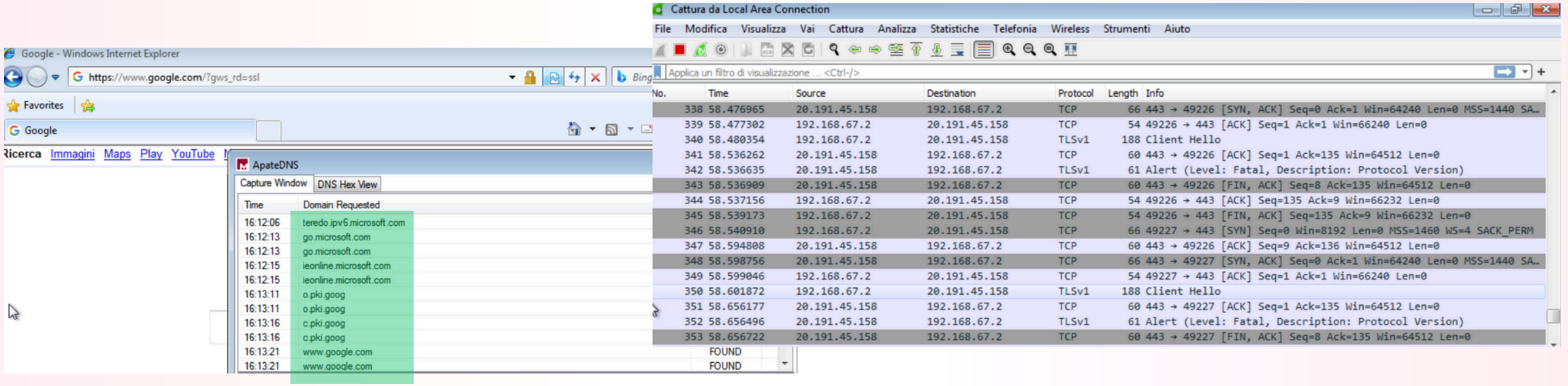
Proviamo a controllare l'eseguibile anche su **CFF Explorer**. E' un browser, quindi è normale che faccia utilizzo massiccio di determinate funzioni. Le sezioni **non sono oscurate**, caso molto difficile per un malware che solitamente tenta di nascondere le sezioni.





ANALISI DINAMICA

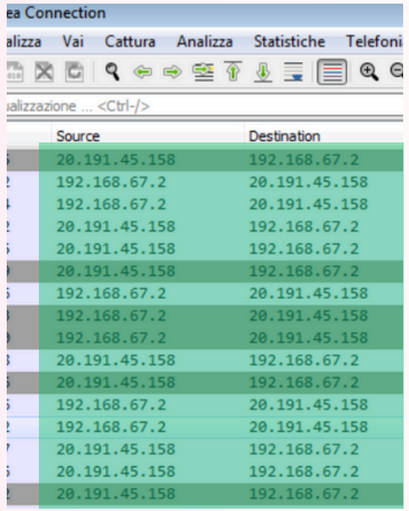
Utilizziamo adesso **apataDNS** per fare da proxy e carpire le richieste di **iexplore.exe,** e Wireshark per intercettare e analizzare il traffico di rete.



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.



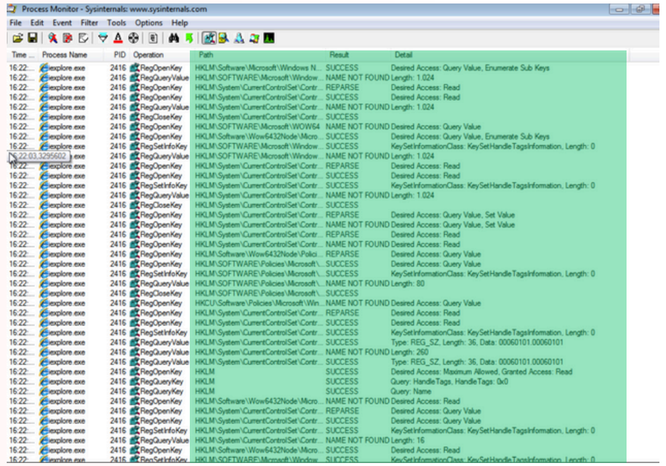

```
flavio@MacBook-Pro ~ % whois 20.191.45.158
% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

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
```

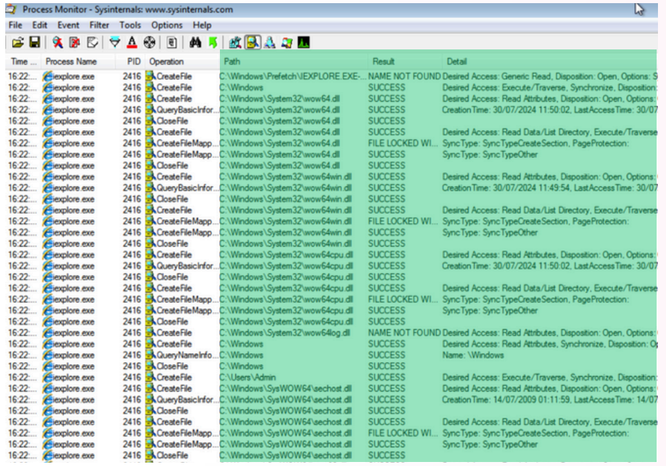
```
flavio@MacBook-Pro ~ % dig 20.191.45.158 MX

; <<>> 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
```

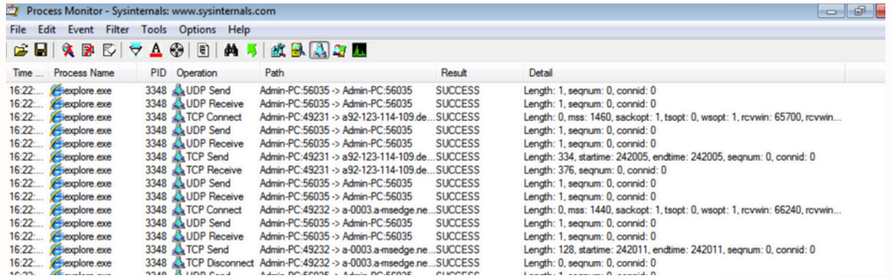
```
flavio@MacBook-Pro ~ % curl -I 20.191.45.158
HTTP/1.1 301 Moved Permanently
Server: Microsoft-Azure-Application-Gateway/v2
Date: Fri, 02 Aug 2024 14:24:55 GMT
Content-Type: text/html
Content-Length: 195
Connection: keep-alive
Location: https://20.191.45.158/
```

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**.







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