

Copia di Esercitazione WEEK 21 D4

Analisi dinamica basica

Ettore Farris

Descrizione sintetica

Traccia:

Un giovane dipendente neo assunto segnala al reparto tecnico la presenza di un programma sospetto.

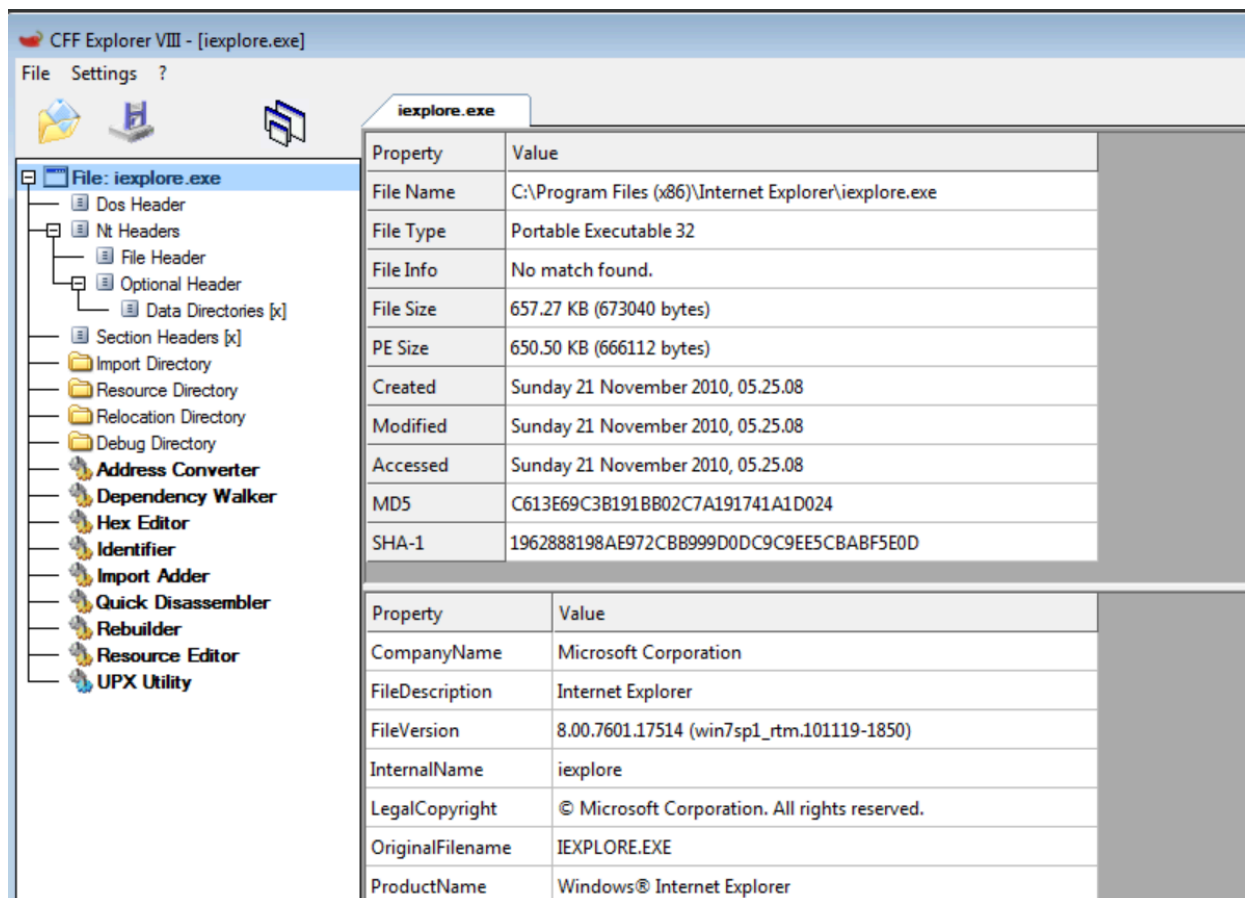
Il suo superiore gli dice di stare tranquillo ma lui non è soddisfatto e chiede supporto al SOC. Il file "sospetto" è IEXPLORE.EXE contenuto nella cartella C:\Program Files\Internet Explorer.

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 è buono.

Svolgimento

- Analisi con CFFExplorer

Per prima cosa, effettuiamo un'analisi statica utilizzando *CFFExplorer* in modo da reperire informazioni sull'eseguibile.



The screenshot shows the CFF Explorer VIII interface. On the left, a tree view displays the file structure of iexplore.exe, including headers, sections, and various directories. The right pane shows the properties of the selected file, iexplore.exe, organized into two tables.

Property	Value
File Name	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	657.27 KB (673040 bytes)
PE Size	650.50 KB (666112 bytes)
Created	Sunday 21 November 2010, 05.25.08
Modified	Sunday 21 November 2010, 05.25.08
Accessed	Sunday 21 November 2010, 05.25.08
MD5	C613E69C3B191BB02C7A191741A1D024
SHA-1	1962888198AE972CBB999D0DC9C9EE5CBABF5E0D

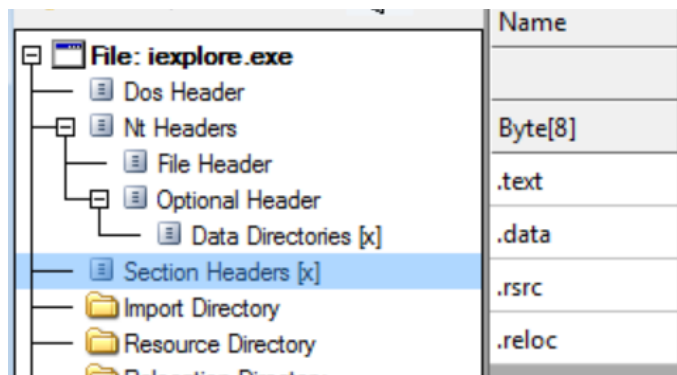
Property	Value
CompanyName	Microsoft Corporation
FileDescription	Internet Explorer
FileVersion	8.00.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	iexplore
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	IEXPLORE.EXE
ProductName	Windows® Internet Explorer

Da questa analisi otteniamo delle informazioni sull'eseguibile come:

- Data di creazione;
- Data di ultima modifica;
- Gli hash MD5 e SHA-1 del programma
- L'azienda creatrice, ovvero Microsoft;
- La versione del file;

- Il nome dell'eseguibile e quello commerciale del prodotto.

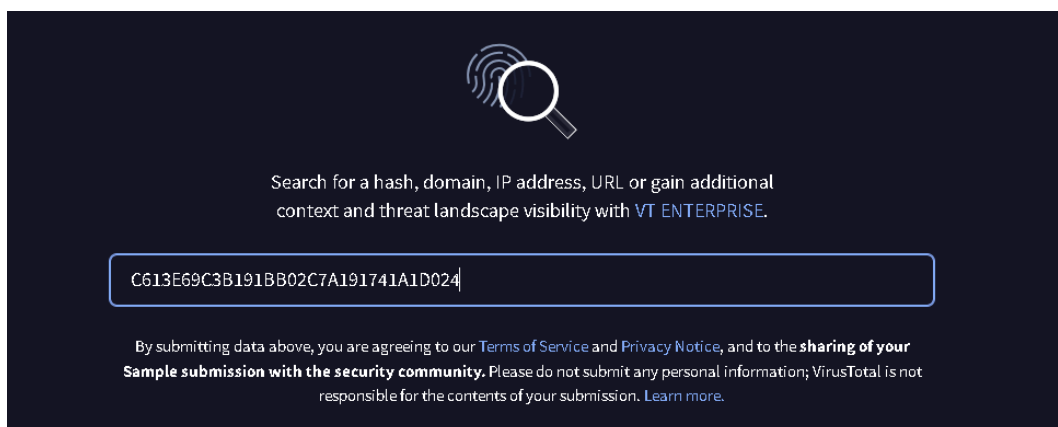
Da CFFExplorer vediamo anche gli headers, le librerie usate dal programma e le funzioni chiamate.



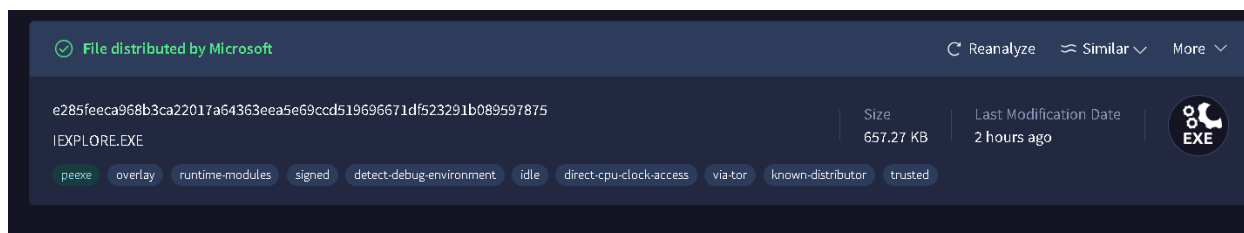
Module Name	Imports	OFfs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	9	0000A518	FFFFFFFF	FFFFFFFF	0000A508	00001000
KERNEL32.dll	59	0000A540	FFFFFFFF	FFFFFFFF	0000A4F8	00001028
USER32.dll	9	0000A630	FFFFFFFF	FFFFFFFF	0000A4EC	00001118
msvcrt.dll	28	0000A658	FFFFFFFF	FFFFFFFF	0000A4E0	00001140
ntdll.dll	1	0000A6CC	FFFFFFFF	FFFFFFFF	0000A4D4	000011B4
SHLWAPI.dll	18	0000A6D4	FFFFFFFF	FFFFFFFF	0000A4C8	000011BC
SHELL32.dll	2	0000A720	FFFFFFFF	FFFFFFFF	0000A4BC	00001208
ole32.dll	2	0000A72C	FFFFFFFF	FFFFFFFF	0000A4B0	00001214
iertutil.dll	14	0000A738	FFFFFFFF	FFFFFFFF	0000A4A0	00001220
urlmon.dll	3	0000A774	FFFFFFFF	FFFFFFFF	0000A494	0000125C

- **Analisi con VirusTotal**

Le informazioni generali trovate con *CFFExplorer* sembrano confermare l'autenticità del file .exe. Per dare ulteriore conferma, andiamo su *VirusTotal* e inseriamo l'hash per vedere se compare nel database.



L'eseguibile sembra attendibile in quanto è presente nel database ed verificato come file Microsoft.



Il file è firmato e controfirmato da più autorità digitali ed ha una firma valida.



La data di creazione e il nome dell'eseguibile della nostra versione (*iexplore.exe*) sembrano coincidere con i dati trovati in precedenza.

History ⓘ	
Creation Time	2010-11-20 09:46:58 UTC
Signature Date	2010-11-20 12:22:00 UTC
First Seen In The Wild	2010-01-15 16:47:01 UTC
First Submission	2011-01-15 15:18:44 UTC
Last Submission	2024-03-02 16:16:31 UTC
Last Analysis	2024-01-01 06:40:35 UTC
Names ⓘ	
iexplore.exe	
IEXPLORE.EXE	
newiexplore.exe	
iexplore.exe.dat	
iexplor.exe	
iexplore.bat.exe	
iexplore.exe_	
ttk.exe	
iexplore.cab	
iexplore	

Gli headers e le librerie usate dall'eseguibile coincidono con quelle trovate con *CFFExplorer*.

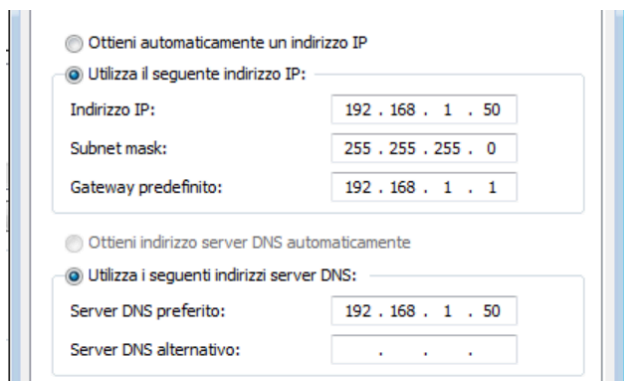
Sections						
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5	Chi2
.text	4096	41093	41472	5.84	90e728188ecf1a607f521e9365e8f3d4	848500.88
.data	49152	1560	1536	0.29	076bf136b6cf6d506f95b5f387da1cc7	370498.41
.rsrc	53248	618528	619008	6.78	e119bb8d564c721091b97ed0d2362a0f	7951474
.reloc	675840	2956	3072	6.36	e1c0ea7a45e2fc4f9df3bcb0d4414d7f	14703.79

Imports	
+ urlmon.dll	
+ iertutil.dll	
+ ADVAPI32.dll	
+ KERNEL32.dll	
+ msvcrt.dll	
+ SHELL32.dll	
+ ntdll.dll	
+ ole32.dll	
+ SHLWAPI.dll	
+ USER32.dll	

- **Analisi con ApateDNS e Wireshark**

Verifichiamo i tentativi di connessione che l'eseguibile effettua appena lanciato per cercare di capire se tenta di contattare siti sospetti, altri host della rete o un C&C Server remoto.

Impostiamo un IP statico e il DNS coincidente a quello della nostra macchina. Sarà lo stesso utilizzato per intercettare le chiamate DNS tramite *ApateDNS*.



☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 1 . 50

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 1 . 1

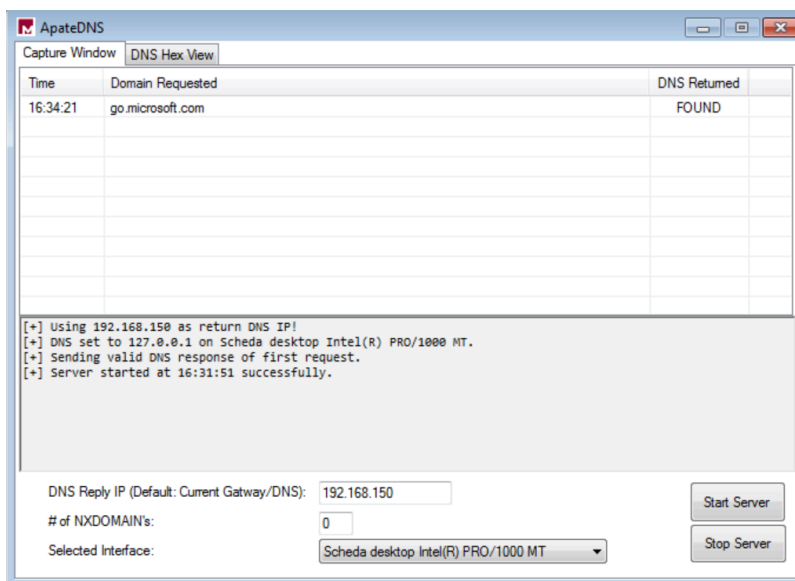
☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

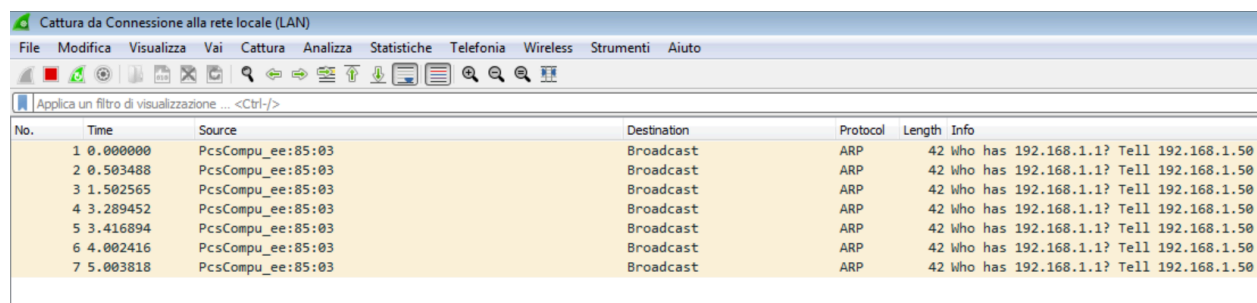
Server DNS preferito: 192 . 168 . 1 . 50

Server DNS alternativo: . . .

Lanciamo poi Wireshark, ApateDNS e, successivamente *iexplore.exe*.



In assenza di internet, *ApateDNS* mostra che Internet Explorer tenta di connettersi solo all'indirizzo *go.microsoft.com*, che è un sito benevolo di proprietà della Microsoft.



The screenshot shows a Wireshark network capture window titled "Cattura da Connessione alla rete locale (LAN)". The interface includes a menu bar (File, Modifica, Visualizza, Vai, Cattura, Analizza, Statistiche, Telefonia, Wireless, Strumenti, Aiuto) and a toolbar. Below the toolbar is a filter bar with the text "Applica un filtro di visualizzazione ... <Ctrl-/>". The main display area shows a list of captured packets. The first seven packets are ARP broadcasts from source "PcsCompu_ee:85:03" to destination "Broadcast". The "Info" column for these packets shows "42 Who has 192.168.1.1? Tell 192.168.1.50".

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
2	0.503488	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
3	1.502565	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
4	3.289452	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
5	3.416894	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
6	4.002416	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50
7	5.003818	PcsCompu_ee:85:03	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.50

Wireshark ci mostra soltanto l'invio di pacchetti ARP di *broadcast* e non restituisce nessuna attività sospetta.

- **Analisi con ProcMon**

Dall'analisi ProcMon non notiamo nessuna attività sospetta riguardo:

- Azioni sul *file system*

Non notiamo nessuna azione sospetta, come la creazione e la manipolazione di files sospetti;

- Eventi di rete

Non notiamo nessun processo che ci riporta a una connessione sospetta.

- Modifica chiavi di registro

Vengono modificate diverse chiavi di registro. Da una prima ricerca, le chiavi modificate rientrano nella normale funzionamento di Internet Explorer.