

Esercitazione W21D4

Malware Analysis: Analisi statica/dinamica basica

Fabio Benevento - 29/03/2024

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.

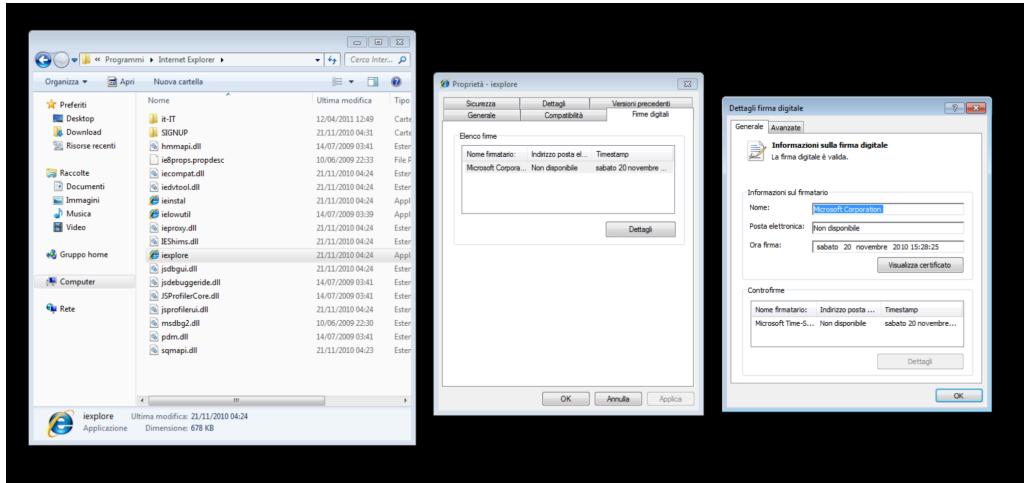
No disassembly no debug o similari VirusTotal non basta, ovviamente.

Non basta dire iexplorer è Microsoft è buono, punto.

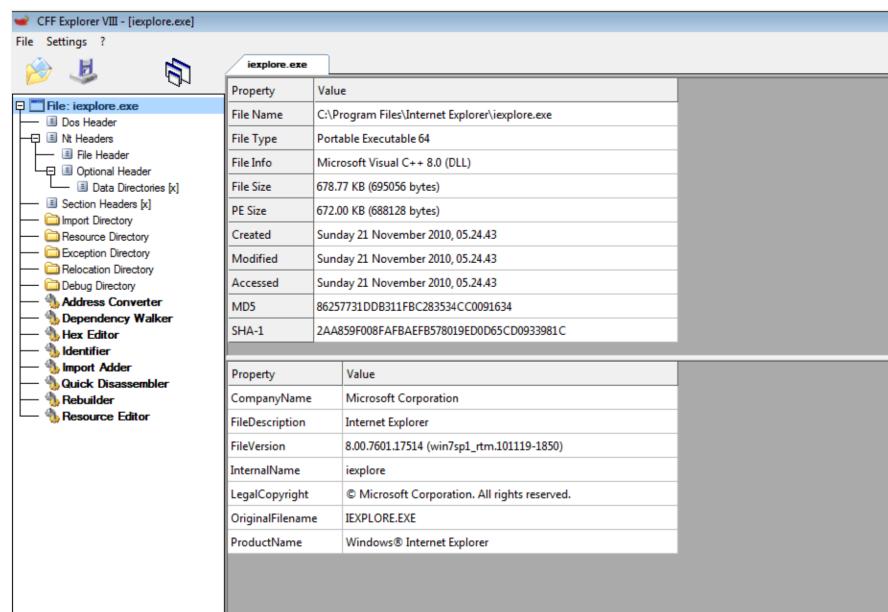
Implementazione

Analisi statica

Come prima analisi sul file Internet Explorer ho verificato la firma digitale del file, la quale sembra in questo caso non sembrare incongruità essendo rilasciata da Microsoft. Si tratta comunque di una chiave di tipo SHA1, oramai superata e facilmente craccabile.



Ho quindi avviato una fase di analisi statica tramite il tool CFF Explorer. Tramite esso è possibile ad esempio vedere che l'eseguibile è stato modificato per l'ultima volta il 21 Novembre 2021 e trovare quella che è la sua chiave.



Utilizzando quest'ultima all'interno del sito VirusTotal è possibile stabilire che si tratta effettivamente di InternetExplorer e che non si tratta di un malware.

Vendor	Result
Acronis (Static ML)	Undetected
Alibaba	Undetected
ALYac	Undetected
Arcabit	Undetected
AhnLab-V3	Undetected
AliCloud	Undetected
Antiy-AVL	Undetected
Avast	Undetected

Ad ulteriore conferma, le informazioni circa le librerie utilizzate sono congruenti tra quelle individuate tramite CFFExplorer e VirusTotal

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000DEA8	N/A	0000DD58	0000DD5C	0000DD60	0000DD64	0000DD68
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
ADVAPI32.dll	13	0000F688	FFFFFFF	FFFFFFF	0000F6A8	00009000
KERNEL32.dll	56	0000F728	FFFFFFF	FFFFFFF	0000F698	00009070
USER32.dll	9	0000F8F0	FFFFFFF	FFFFFFF	0000F68C	00009238
msvcrtdll	29	0000F940	FFFFFFF	FFFFFFF	0000F680	00009288
ntdll.dll	3	0000FA30	FFFFFFF	FFFFFFF	0000F674	00009378
SHLWAPI.dll	23	0000FA50	FFFFFFF	FFFFFFF	0000F668	00009398
SHELL32.dll	7	0000FB10	FFFFFFF	FFFFFFF	0000F65C	00009458
ole32.dll	5	0000FB50	FFFFFFF	FFFFFFF	0000F650	00009498
iertutil.dll	14	0000FB80	FFFFFFF	FFFFFFF	0000F640	000094C8
urlmon.dll	3	0000FBF8	FFFFFFF	FFFFFFF	0000F634	00009540

Header						
Target Machine	x64					
Compilation Timestamp	2010-11-20 10:29:39 UTC					
Entry Point	5156					
Contained Sections	6					
Sections						
Name	Virtual Address	Virtual Size	Raw Size	Entropy	MDS	Chi2
.text	4096	29513	29696	6.2	2bf875dbe0e183d6bc207fa0ebb6902f	232815.58
.rdata	36864	31752	32256	3.49	7ee8b8ad27ce37b115c2ed3bb63ed44a	3238909.25
.data	69632	2828	2560	0.2	3045703bc99a7e139c6bfbef9868f207	629977.38
.pdata	73728	1380	1536	4.23	212a80b5268ff7fd814c9ad19eb9c8	95655.37
.rsrc	77824	618928	619008	6.78	3b1ab9f02eb946a3c987e5fc326ec8b	7951576.5
▼						
Imports						
+ ADVAPI32.dll						
+ KERNEL32.dll						
+ USER32.dll						
+ msvert.dll						
+ ntdll.dll						
+ SHLWAPI.dll						
+ SHELL32.dll						
+ ole32.dll						
+ iertutil.dll						
+ urlmon.dll						

Analisi Dinamica

Per eseguire l'analisi dinamica, ho avviato e configurato i tool ProcMon, ApateDns e Regshot quindi ho avviato Internet Explorer per effettuare l'analisi. Nello specifico ho configurato ApateDns con l'indirizzo ip della macchina in maniera da rispondere e sostituirsi al dns di default, mentre in Regshot ho acquisito la cattura dei registri di sistema prima dell'avvio dell'applicazione per il successivo confronto.

Procmon

Analizzando la cattura delle operazioni eseguite dal processo iexplorer in seguito al suo avvio, non si rilevano operazioni sospette. Il processo accede a directory e file sotto il proprio path ed accede e modifica chiavi di registro del tutto lecite.

Regshot

Effettuando una nuova cattura in regshot (2st shot) è possibile poi effettuare il confronto tra le due catture e verificare le chiavi di registro modificate indicate nel report generato. Esse ricalcano le operazioni di scrittura sul registro già individuate in procmon e come detto in precedenza non destano particolare allarmi.

ApateDns

Mediante ApateDns è possibile individuare i tentativi di accesso effettuati dall'applicazione a specifici indirizzi di rete.

Anche in questo caso, analizzando gli host contattati, sono tutti indirizzi leciti che non destano particolari sospetti.

The screenshot shows the ApateDNS application window. At the top, there are two tabs: "Capture Window" (selected) and "DNS Hex View". Below the tabs is a table with columns "Time", "Domain Requested", and "DNS Returned". The table contains the following data:

Time	Domain Requested	DNS Returned
17:07:39	go.microsoft.com	FOUND
17:08:32	www.google.it	FOUND
17:08:33	www.bing.com	FOUND
17:09:19	go.microsoft.com	FOUND
17:09:32	www.google.it	FOUND
17:09:33	www.bing.com	FOUND
17:18:35	firefox.settings.services.mozilla.com	FOUND
17:24:46	time.windows.com	FOUND

Below the table is a log window containing the following text:

```
[+] Using 192.168.50.120 as return DNS IP!
[+] DNS set to 127.0.0.1 on Scheda desktop Intel(R) PRO/1000 MT.
[+] Sending valid DNS response of first request.
[+] Server started at 16:53:17 successfully.
```

At the bottom of the window, there are configuration options and control buttons:

- DNS Reply IP (Default: Current Gateway/DNS):
- # of NXDOMAIN's:
- Selected Interface:
- Start Server (blue button)
- Stop Server (gray button)