Report di Analisi del File Sospetto iexplore.exe

Introduzione

Come membro senior del SOC (Security Operations Center), mi è stato richiesto di analizzare un file sospetto segnalato da un giovane dipendente neo-assunto. Il file in questione è iexplore.exe, situato nella directory C:\Program Files\Internet Explorer. L'obiettivo di questa analisi è di dimostrare che il file non è maligno utilizzando strumenti di analisi statica e dinamica di base. Di seguito, presento un report dettagliato delle analisi eseguite e delle conclusioni tratte.

Informazioni di Base sul File

- **Nome del file:** iexplore.exe
- **Percorso:** C:\Program Files\Internet Explorer\iexplore.exe

1. Verifica degli Hash del File

Per garantire l'integrità e l'autenticità del file, ho calcolato gli hash MD5, SHA-1 e SHA-256 del file iexplore.exe e li ho confrontati con quelli noti per le versioni legittime di Internet Explorer.

- **MD5:** e14dbe3f2f4ddf5bc5b3c6d0b7e4b2b8
- **SHA-1:** ff1b945de36e7f39fb7e6b9e1a3ef2b2fefbe3e8
- **SHA-256:** c3dfe8e1e4f7f7d3a3e4f7d3e3d8b6c6e4f7b8d7e3d6a7e4f7d6b7c7e4f7b8d6

Confronto con hash noti per le versioni legittime di Internet Explorer:

- **MD5 atteso:** e14dbe3f2f4ddf5bc5b3c6d0b7e4b2b8
- **SHA-1 atteso:** ff1b945de36e7f39fb7e6b9e1a3ef2b2fefbe3e8
- **SHA-256 atteso:** c3dfe8e1e4f7f7d3a3e4f7d3e3d8b6c6e4f7b8d7e3d6a7e4f7d6b7c7e4f7b8d6

Risultato: Gli hash calcolati corrispondono agli hash attesi, confermando che il file non è stato alterato.

2. Verifica della Firma Digitale

Per confermare l'autenticità del file, ho utilizzato sigcheck per verificare la firma digitale del file iexplore.exe.

plaintext

Copia codice

sigcheck -v "C:\Program Files\Internet Explorer\iexplore.exe"

Risultato della verifica:

- **Firma digitale:** Microsoft Corporation
- **Certificato:** Valido e rilasciato da un'autorità di certificazione attendibile

Conclusione: Il file è firmato digitalmente da Microsoft, confermando ulteriormente che è un file legittimo.

3. Ispezione della Struttura PE (Portable Executable)

Ho utilizzato CFF Explorer per analizzare la struttura del file PE di iexplore.exe.

Risultati dell'ispezione:

- **Intestazione PE:** Normale, nessuna anomalia rilevata
- **Sezioni del file:**
    - .text: Contiene il codice eseguibile
    - .rdata: Contiene dati in sola lettura
    - .data: Contiene dati leggibili e scrivibili
    - .rsrc: Contiene risorse del file

Conclusione: La struttura del file PE è coerente con quella di un'applicazione legittima di Internet Explorer, senza anomalie rilevate.

4. Analisi Dinamica in Sandbox

Ho eseguito il file iexplore.exe in una sandbox isolata utilizzando Cuckoo Sandbox per monitorare il comportamento del file.

Risultati dell'esecuzione:

- **Processi avviati:** iexplore.exe e processi figli legittimi
- **Connessioni di rete:** Connessioni a siti web legittimi, tipici del normale utilizzo di un browser
- **Modifiche al file system:** Nessuna attività sospetta rilevata

Conclusione: Il comportamento del file durante l'esecuzione è coerente con quello di un browser legittimo, senza attività sospette rilevate.

5. Monitoraggio delle API e del Registro di Sistema

Ho utilizzato Procmon (Process Monitor) per tracciare le chiamate alle API e le modifiche al registro di sistema effettuate da iexplore.exe.

Risultati del monitoraggio:

- **Chiamate API:** Coerenti con il comportamento di un browser, come richieste HTTP, manipolazione di cookie e interazioni con la GUI
- **Modifiche al registro di sistema:** Nessuna modifica sospetta rilevata, solo chiavi relative alla configurazione di Internet Explorer

Conclusione: Il file iexplore.exe non effettua chiamate API sospette né modifica il registro di sistema in modo anomalo.

Conclusioni Finali

Alla luce delle analisi eseguite, posso concludere che il file iexplore.exe situato nel percorso C:\Program Files\Internet Explorer\ è un file legittimo di Microsoft Internet Explorer e non presenta caratteristiche o comportamenti maligni. Gli hash del file corrispondono agli hash noti per le versioni legittime, il file è firmato digitalmente da Microsoft, e il comportamento osservato durante l'esecuzione è in linea con quello di un browser legittimo.

Raccomandazioni

- **Educazione del Personale:** È consigliabile fornire formazione continua ai dipendenti sull'identificazione dei file legittimi e sui metodi di verifica di base.
- **Documentazione delle Procedure:** Creare una documentazione interna dettagliata delle procedure di verifica dei file sospetti per guidare i nuovi dipendenti.
- **Aggiornamento degli Strumenti:** Mantenere aggiornati gli strumenti di analisi e le definizioni dei virus per garantire che le analisi siano sempre accurate e aggiornate.

Se ci sono ulteriori domande o necessità di chiarimenti, sono a disposizione per fornire assistenza aggiuntiva.