Pratica S10/L2

Traccia:

Configurare la macchina virtuale per l'analisi dinamica (il malware sarà effettivamente eseguito).

Con riferimento al file eseguibile contenuto nella cartella «**Esercizio_Pratico_U3_W2_L2**» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor (procmon)
- Identificare eventuali azioni del malware su **processi e thread** utilizzando Process Monitor
- Modifiche del registro dopo il malware (**le differenze**)
- Provare a profilare il malware in base alla correlazione tra «operation» e Path.

In questo esercizio viene fatta un'**analisi dinamica basica**, che comprende tutte quelle attività di analisi che presuppongono l'esecuzione del malware in un ambiente dedicato.

Per questa analisi sono stati utilizzati i seguenti tools:

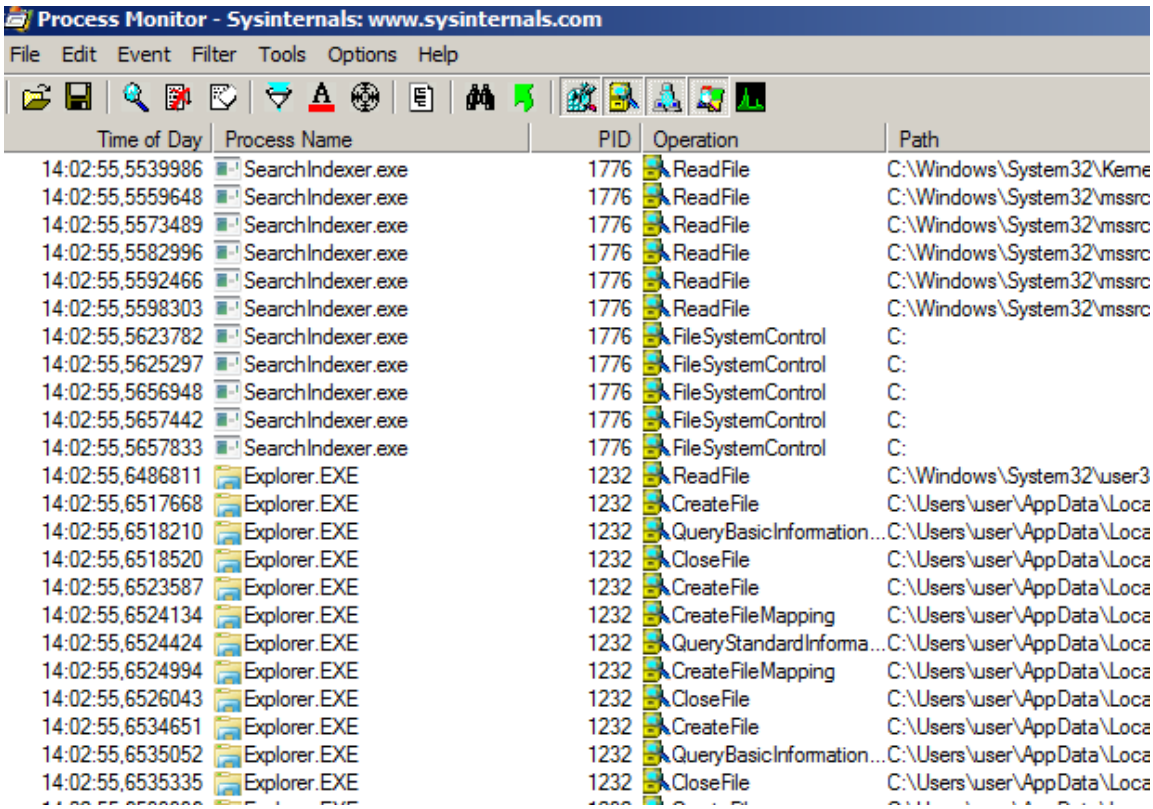
- **Regshot**: permette di paragonare due istantanee delle chiavi di registro salvate in due momenti separati tra di loro;
- **Process Monitor o procmon**: permette di monitorare i processi ed i thread attivi, l'attività di rete, l'accesso ai file e le chiamate di sistema effettuate su un sistema operativo.

Le chiavi di registro riflettono le configurazioni del sistema operativo. Quelle più importanti sono:

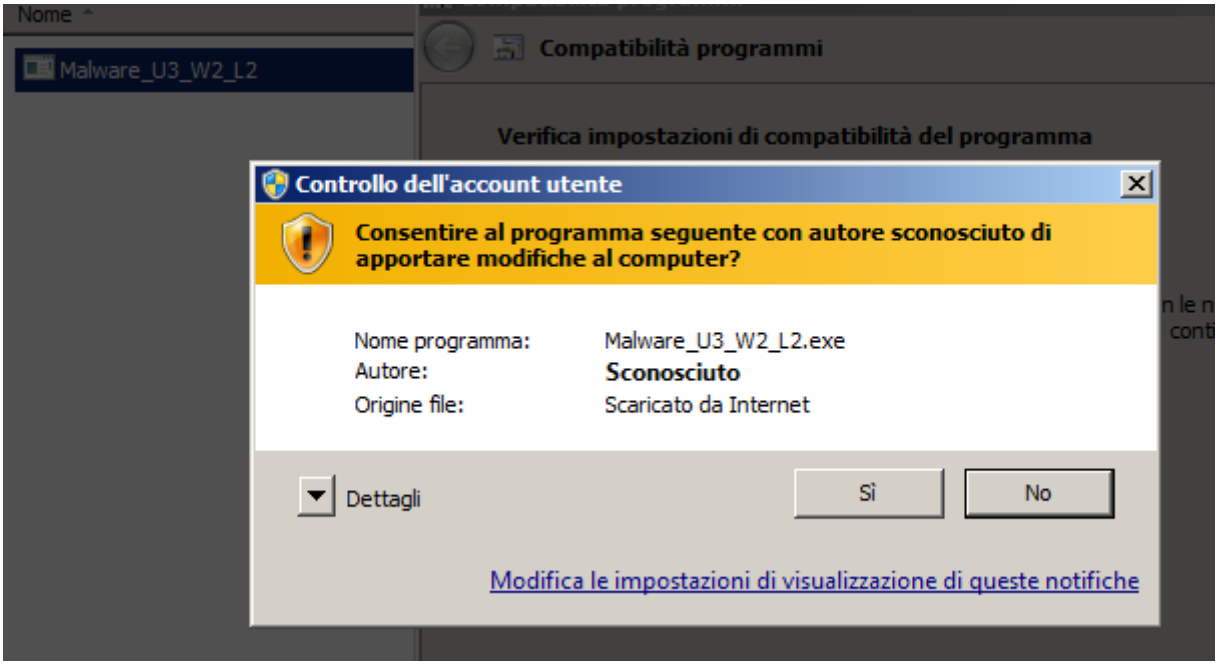
- **HKEY_CURRENT_USER (HCU)**: include le impostazioni e preferenze di sistema dell'utente collegato;
- **HKEY_LOCAL_MACHINE (HKLM)**: include le impostazioni comuni per tutti gli utenti del sistema;
- **HKEY_USERS (HKU)**: raggruppa le impostazioni di tutti gli utenti.

Creata una 1° istantanea con «**Regshot**» da comparare successivamente dopo l'esecuzione del marware.

Avvio di «**Process Monitor**»



Esecuzione del **Malware**



Dopo pochi secondi l'esecuzione del file sono stati fermati il programma **Process Monitor** e creata una 2° istantanea con **Regshot**.

Identificare eventuali azioni del malware sul **file system**

Per l'attività del malware sul File System mi sono soffermato sull'Operation CreateFile del percorso dell'eseguibile. Si è riscontrato che il malware ha creato del file all'interno di alcuni processi fondamentali del sistema operativo:

- **explorer.exe**: fornisce l'interfaccia GUI del sistema operativo;
- **svchost.exe**: può ospitare uno o più processi del sistema operativo Windows;
- **conhost.exe**: interfaccia utente per l'uso delle applicazioni da riga di comando;
- **sdiagnhost.exe**: essenziale per il corretto funzionamento delle applicazioni;
- **taskeng.exe**: permette al sistema operativo di avviare programmi o script in momenti specifici o dopo un lasso di tempo programmato;
- **consent.exe**: parte dell'applicazione Controllo Utente e avvia l'interfaccia per Windows UAC (User Account Controll).

Identificare eventuali azioni del malware su **processi e thread**

Le modifiche ha il malware ha apportato ai processi e thread sono:

- **Thread Create**: crea dei flussi di istruzione, all'interno del processo, che possono essere eseguiti separatamente o contemporaneamente;
- **Load Image**: carica eseguibili e librerie;
- **Process Create**: Crea nuovi processi.

Modifiche del registro dopo il malware

Le modifiche del registro di sistema, dopo l'esecuzione del malware, risultano essere per un totale di 95, di cui:

- 6 HKLM cancellate;
- 8 HKLM aggiunte;
- 38 HKLM valori cancellati;
- 2 HKU valori cancellati;
- 12 HKLM valori aggiunti;
- 2 HKU valori aggiunti;
- 12 HKLM valori modificati;
- 15 HKU valori modificati.

Provare a profilare il malware in base alla correlazione tra «operation» e Path

La creazione dei processi può portare acquisizione dei privilegi di amministratore per aggirare i controlli di sicurezza, permettendo di:

- Rubare password e dati;
- Scaricare altri malware;
- Prendere il controllo del computer;
- Creare backdoor per l'accesso remoto;
- Monitorare e modificare le impostazioni di sistema;
- Disattivare il software di sicurezza;
- Distribuire Ransomware tra i file.