Nell’esercizio di oggi ci viene chiesto di:

-Identificare eventuali azioni del malware sul file system utilizzando Process Monitor (procmon)

-Identificare eventuali azioni del malware su processi e thread utilizzando Process Monitor

-Individuare modifiche del registro dopo il malware (le differenze)

L'analisi dinamica di un malware è un processo che coinvolge l'esecuzione del malware in un ambiente controllato per osservare il suo comportamento in tempo reale.

Quest’analisi segue alcuni step fondamentali:

- **Preparazione dell'ambiente**: Prima di eseguire il malware, è necessario preparare un ambiente sicuro e controllato, ad esempio una macchina virtuale o una sandbox. Questo ambiente dovrebbe essere isolato dalla rete e da altri sistemi critici per prevenire la diffusione del malware.

- **Esecuzione del malware**: Una volta che l'ambiente è pronto, il malware viene eseguito. Durante l'esecuzione, vengono registrate tutte le attività del malware, inclusi i file che crea, le modifiche al registro di sistema, le connessioni di rete che tenta di stabilire e altre azioni dannose.

- **Monitoraggio delle attività**: Durante l'esecuzione del malware, gli analisti monitorano attentamente le attività del sistema per individuare comportamenti sospetti o dannosi. Questo può includere l'analisi del traffico di rete, la registrazione delle attività del processo e l'osservazione delle modifiche ai file di sistema.

- **Analisi del comportamento**: Gli analisti esaminano il comportamento del malware per comprendere le sue funzionalità e gli obiettivi. Possono cercare di rispondere a domande come: quali file vengono modificati o creati? Quali processi vengono avviati? A quali risorse di sistema o di rete tenta di accedere il malware?

- **Raccolta di indicatori di compromissione (IOCs)**: Durante l'analisi dinamica, vengono raccolti indicatori che possono essere utilizzati per identificare il malware o rilevare la sua presenza in futuro. Questi possono includere hash del file, indirizzi IP, URL, nomi di file e altro ancora.

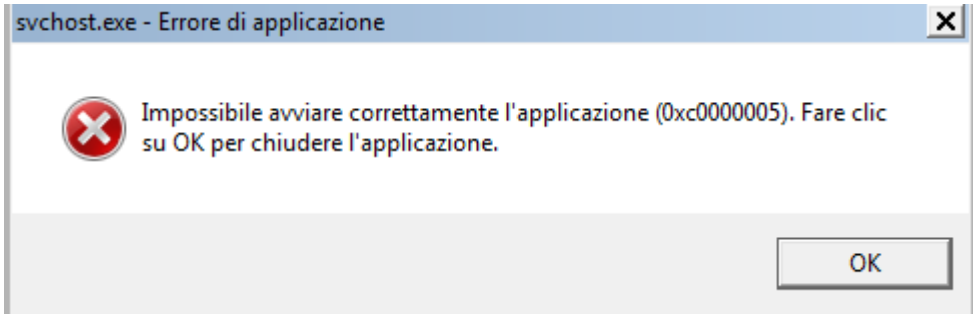
- **Generazione di firme e regole di rilevamento**: Basandosi sull'analisi del comportamento e sugli IOCs raccolti, gli analisti possono generare firme e regole di rilevamento per aiutare a identificare e bloccare il malware su altri sistemi.

L’analisi dinamica di un malware prevede l’avviamento del malware e un monitoraggio tramite tool vari;

per esempio per l’analisi delle modifiche alle chiavi di registro del sistema utilizziamo Process Monitor, mentre per analizzare le richieste remote su internet si utilizza Apate DNS.

Tuttavia non è stato possibile avviare il malware poiché questi utilizza delle librerie che sono obsolete su windows 7, ma vrebbero funzionato invece su Windows XP.

Quando tentiamo di avviare il malware da Windows 7 ci compare il seguente Messaggio di errore:



Windows ha sicuramente deciso di non utilizzare piu alcune delle librerie presenti su windows XP poiché sarebbe stato possibile per un malware sfruttare queste vulnerabilità per caricare da remoto file malevoli o inviare informazioni sulla macchina.