

The background features a dark blue gradient with three glowing, translucent toroidal rings. One ring is positioned behind the title text, another is to the right, and a partial third ring is visible at the bottom left.

# **Analisi dinamica basica**



# Introduzione

In questo documento descrivo il processo di configurazione di una macchina virtuale per l'analisi dinamica basica di un malware, evidenziando le difficoltà incontrate e i problemi di compatibilità riscontrati. Il malware in questione si trova nella cartella "Esercizio\_Pratico\_U3\_W2\_L2" presente sul desktop della macchina virtuale dedicata all'analisi dei malware.



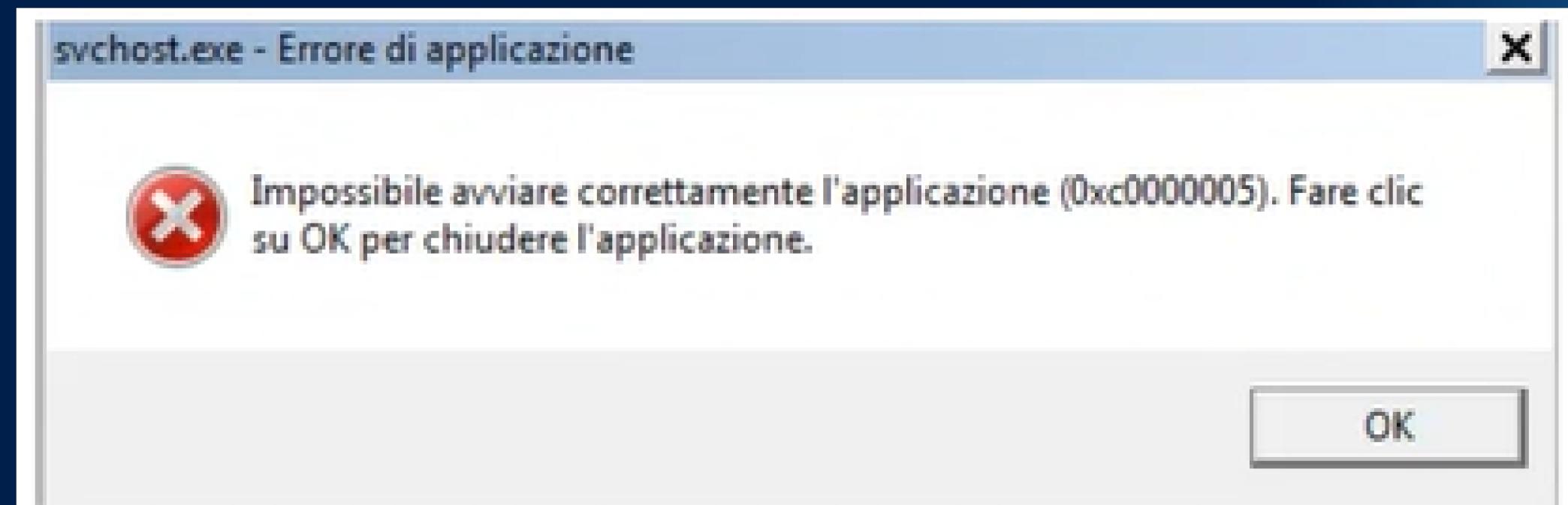
# Configurazione della Macchina Virtuale

Per condurre un'analisi dinamica, ho configurato una macchina virtuale con Windows 7 disabilitando ogni possibile comunicazione tra la mia macchina e la macchina virtuale, per impedire al malware la possibilità di propagarsi.

Per effettuare l'analisi userò principalmente Process Monitor (ProcMon) per monitorare in tempo reale il file system, il registro di sistema e l'attività dei processi/thread.

# Esecuzione del Malware

Dopo aver preparato l'ambiente, ho avviato il malware eseguibile dalla cartella "Esercizio\_Pratico\_U3\_W2\_L2". Tuttavia, subito dopo l'avvio, è apparso il seguente messaggio di errore:



# Descrizione del Problema

Questo errore è dovuto al fatto che il malware utilizza librerie obsolete compatibili con Windows XP, mentre io sto utilizzando Windows 7. L'errore 0xc0000005 indica solitamente un problema di accesso alla memoria, spesso causato da incompatibilità con le librerie o le API di sistema.

L'analisi dinamica non è stata possibile a causa dell'errore di compatibilità. Questo evidenzia l'importanza di utilizzare un ambiente appropriato per l'esecuzione di malware, soprattutto quando si tratta di eseguibili che potrebbero essere stati sviluppati per versioni di Windows obsolete.