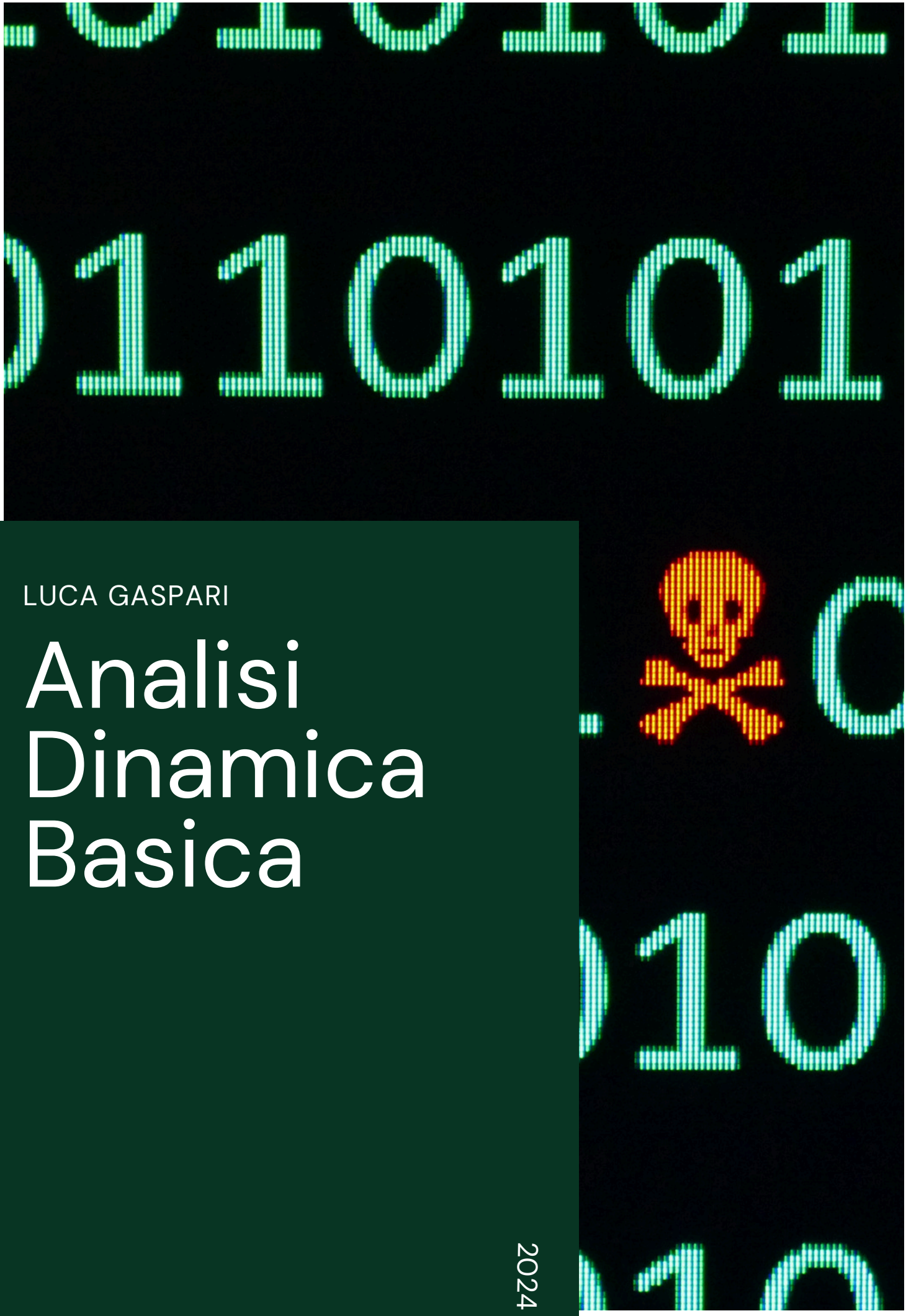

LUCA GASPARI

Analisi Dinamica Basica

2024

Traccia esercizio S10L2

EPICODE | Pratica S10/L2 PDF | Esercizio — Analisi dinamica

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.

L'esercizio è volto ad eseguire un'analisi dinamica basica con l'esecuzione del malware all'interno di un ambiente controllato per osservare e documentare il suo comportamento. Nello specifico, l'esercizio richiede l'uso di Process Monitor (procmon) per monitorare le azioni del malware sul file system, sui processi e thread, e le modifiche al registro di sistema..

Purtroppo, l'esercizio non può essere svolto nella sua forma attuale a causa delle patch di aggiornamento che hanno reso non funzionante il malware fornito, questo è un problema comune nella ricerca e analisi dei malware, dove gli aggiornamenti di sicurezza possono alterare il comportamento del malware o impedirne l'esecuzione.