Artifact template

A04 – Infected document

ID	**A04 – Infected document**
Category	Malware analysis
Difficulty	Easy
Description (This text could be shared with the participants if necessary)	
Additional material	Word document
Technical requirements/ others	None
Preparation	
Resolution	In this challenge, the participant receives what appears to be a regular PDF file. In reality, it is an executable file created to infect all executables found in the current directory with a ransomware. After that, it then opens the embedded PDF file, so that the user initially notices nothing. To avoid real risks, the script is fully operational, but simply renames the .exe files with an 'INFECTED' suffix. The participant's mission will be to discover this trick, analyse its functioning and conclude that this was the means of infection and propagation used.