Artifact template

A11 – Wiper malware

ID	**A11 - Wiper malware**
Category	Malware analysis
Difficulty	Hard
Description (This text could be shared with the participants if necessary)	
Additional material	Executable (sn00ker.exe)
Technical requirements/ others	None
Preparation	
Resolution	In this challenge, participants must disassemble and analyse an executable that has been found among the files left by the attackers. This executable, written in C, searches for all files on the hard disk with a 'tar.gz' or 'zip' extension and deletes them. For security reasons, the executable actually provided to the participants does not actually delete the files, but renames them, including the suffix 'DELETED'. The mission of the participants will be to analyse the executable, discover its behaviour and, specifically, that it was designed to delete the backups (.tar.gz and .zip extensions).