**Question 1: Examining the Malware**

Unveiling the Intricacies: Malware Analysis Report on a Simple Python-Based Threat

This report explores a malicious Python script that modifies files and folders. Malicious files are concealed in designated directories and pre-existing files are duplicated with altered filenames, which are the two primary ways the malware propagates. To conceal its presence, the 'create\_new\_malware()' technique subtly duplicates itself in directories ending in ".malware.py". Concurrently, the 'copy\_existing\_files()' function modifies filenames in a methodical manner, causing modified copies of files that are not hidden. Using this tactic, the malware is categorised as a File and Directory Infector that is adept at hiding its existence.

The malware uses two strategies to increase its elusiveness. By secretly duplicating itself and using a dot-initiated filename, "create\_new\_malware()" lessens its visibility inside directories. Meanwhile, 'copy\_existing\_files()' creates updated versions of files with dots and numerical indices by methodically copying and modifying them. Security experts find it more difficult to identify and mitigate because of the multi-layered obfuscation.

There are serious security dangers associated with the malicious code since it manipulates files and folders without authorization. Because of the malware's ability to proliferate and work smoothly with directories, making detection more difficult, vigilant security measures are important. Several safety measures are advised to reduce threats, including frequent antivirus software upgrades, regular directory searches for strange files, careful review of system logs, and user instruction on handling files carefully. By putting these precautions in place, defences against the malware's possible effects are strengthened. To avoid the use or propagation of malware, this report highlights the harmful nature of the Python code and emphasises the necessity of proactive security measures and user knowledge while abiding by legal and ethical requirements.

**Question 2: Anti-Malware Script**

Explanation of Markers:

1. **"create\_new\_malware"**: Indicates the creation of a new malware file.
2. **"copy\_existing\_files"**: Suggests the replication of existing files.
3. **".malware.py"**: Represents the presence of a hidden malware file.
4. **"list\_directories"**: Indicates the use of directory listing, potentially for propagation.
5. **"self.path =path"**: Suggests manipulation of file paths.