Analysis Report for: powershell.txt

Overall Functionality

This code appears to be a malicious script disguised as PowerShell (due to the syntax) aiming to install a Linux distribution (likely Ubuntu) within Windows using the Windows Subsystem for Linux (WSL). It downloads a compressed Ubuntu distribution, extracts it, installs it using WSL, and then executes two additional executables, `Emblink.exe` and `Embfont.exe`, which are hidden afterward. The script manipulates Windows settings to enable WSL and Virtual Machine Platform features and checks for compatibility.

Function Summaries

The code doesn't contain C functions in the traditional sense. It uses a PowerShell-like syntax. The `Check-WSLCompatibility` function is the only defined piece resembling a function:

* **`Check-WSLCompatibility`**: This function checks if WSL and (if the build number is sufficiently high) the Virtual Machine Platform are enabled on the system. It returns `$true` if both are enabled (or if only WSL is enabled on older systems) and `$false` otherwise. It doesn't take any parameters.

Control Flow

The script's control flow is straightforward, proceeding linearly with conditional checks at various stages:

1. **Download Ubuntu:** If the Ubuntu archive doesn't exist locally, it downloads it from a remote URL.
2. **WSL and Virtual Machine Platform Enablement:** It attempts to enable WSL and the Virtual Machine Platform using DISM commands.
3. **Compatibility Check:** The `Check-WSLCompatibility` function determines whether the necessary features are enabled. The script doesn't explicitly handle the case where the check fails.
4. **Ubuntu Installation:** It creates a directory for the Ubuntu installation, extracts the downloaded archive, and then uses the `wsl` command to import and install the distribution.
5. **Executable Execution and Hiding:** It hides four executables (`Emblink.exe` and `Embfont.exe` in both user and system temp directories) by setting their attributes to 'Hidden' and 'System'. Then it executes either the user or system version of `Emblink.exe` and `Embfont.exe` depending on whether the user version exists, implying a fallback to a system location.
6. **Sleep:** It pauses execution for 30 seconds.

Data Structures

The script uses simple variables to store file paths, strings, and the results of commands. There's no complex data structure usage. The `$filesToHide` variable is an array of strings representing file paths.

Malware Family Suggestion

Based on its behavior, this script strongly suggests a **downloader/installer for malware**. The download of an archive from a suspicious URL, the installation of a Linux distribution (potentially used for persistence or to provide a platform for additional malware), and the subsequent execution of hidden executables (`Emblink.exe` and `Embfont.exe`) are all hallmarks of malicious activity. The executables are likely to perform further malicious actions such as data exfiltration, keylogging, or establishing remote access. The use of PowerShell and obfuscation through spacing and capitalization further supports its malicious nature. This malware falls into the category of **backdoor trojans** or potentially a **RAT (Remote Access Trojan)**, given the potential for persistence and remote control established by the hidden executables.