Analysis Report for: new 1.txt

This code is written in PowerShell, not C. The fact that it was submitted as C code, and the presence of null characters within the provided text strongly suggests an attempt to obfuscate the script. Let's analyze it as PowerShell.

Overall Functionality

This PowerShell script appears to be designed to install and configure the Windows Subsystem for Linux (WSL), potentially downloading a Ubuntu distribution from a potentially malicious URL. Following the WSL installation, it attempts to execute two further executables (`Emblink.exe` and `Embfont.exe`) located in both user and system temporary directories, hiding these executables afterwards. The script manipulates execution policies to run without restrictions. This strongly suggests malicious intent.

Function Summaries

The script doesn't define functions in the traditional sense but uses PowerShell cmdlets and constructs to achieve its goals. The `Check-WSLCompatibility` section acts as a function-like block.

* **Check-WSLCompatibility**: This block checks if WSL and the Virtual Machine Platform are enabled. It returns `$true` if both are enabled and the OS build is 2004 or later; otherwise, it returns `$false`. No parameters are explicitly passed, relying on internal cmdlets to retrieve system information.

Control Flow

1. **Execution Policy Setting**: The script begins by bypassing execution policies (`Set-ExecutionPolicy`). This allows the script to run even if execution policies are set to prevent potentially dangerous scripts. This is a major red flag for malicious behavior.

2. **WSL and Virtual Machine Platform Enabling**: It uses `DISM` to enable WSL and the Virtual Machine Platform if they aren't already enabled.

3. **Ubuntu Download (if needed)**: It checks if `Ubuntu.tar.gz` exists; if not, it downloads it from a suspicious URL (`https://4533f9dd.sgp1.vultr.objects.com/Ubuntu.tar.gz`). The URL's structure hints at it being a dynamically created link on a cloud storage service. This is extremely suspicious.

4. **WSL Compatibility Check**: The `Check-WSLCompatibility` block is executed. This step determines if the system environment supports the script's subsequent actions.

5. **Ubuntu Installation**: If the compatibility check passes, the script proceeds to extract the downloaded `Ubuntu.tar.gz` and runs `wsl --import` to install the Ubuntu distribution.

6. **Executable Execution and Hiding**: After WSL (potentially) installation, the script attempts to run `Emblink.exe` and `Embfont.exe` from either the user's or system's temporary directory, depending on whether the respective file exists. The executables are then hidden using `Get-Item`. The choice of temporary directories hints at the possibility of persistence in the system.

7. **Sleep**: A 30-second sleep is introduced before the script terminates. This might allow time for the malicious executables to perform their actions before the script exits.

Data Structures

The script uses several PowerShell variables to store file paths, strings, and boolean values. There is no explicit use of complex data structures. The `$filesToHide` variable uses an array to store paths to files to hide.

Malware Family Suggestion

Given its functionality, this script exhibits characteristics of several malware families:

* **Downloader/Dropper:** It downloads and executes additional files (`Emblink.exe`, `Embfont.exe`) from a remote server. These could contain any payload—ransomware, backdoors, keyloggers, etc.
* **Installer (potentially backdoored):** It installs WSL, potentially as a cover for installing the malicious payload.
* **Rootkit-like behavior:** It attempts to hide the presence of the executed files.
* **Information Stealer (potential):** The information gathered (build number, etc.) could be sent back to a C2 server to profile the infected system.

The use of obfuscation techniques (null characters in the original submission) reinforces the suspicion that this is malicious. The download URL is particularly alarming, pointing to a potentially malicious and untrusted source. Without further analysis of `Emblink.exe` and `Embfont.exe`, we cannot definitively classify this as a specific malware family, but its behavior strongly suggests malicious intent. Extreme caution is warranted. Never run scripts obtained from untrusted sources or containing obfuscation.