LOLBins Analyzer

Paste suspicious commands below to analyze potential LOLBin abuse.

Suspicious Commands

```
rundll32.exe C:\Users\Public\Document\file.dll,RS32
rundll32.exe C:\programdata\putty.jpg,Wind
```

Analyze

Analysis Result:

The first command, "rundll32.exe C:\\Users\\Public\\Document\\file.dll,RS32" is potentially indicative of LOLBin abuse. This command is using the rundll32.exe executable, which is a legitimate Windows process used for running 32-bit Dynamic Link Libraries (DLLs). However, the path of the DLL being run is suspicious as it is located in the Public folder, which is not a common location for DLLs. This could suggest that the DLL is not a legitimate Windows file and may be malicious or potentially used for nefarious purposes.

The inclusion of the "RS32" argument in the command is also concerning. This argument is not a valid command for the rundll32.exe process and could potentially be a command used by an attacker to execute malicious code hidden within the DLL file. This is a common tactic used in LOLBin abuse, where legitimate system processes are used to hide malicious activity.