Masquerading: Space after Filename, Sub-technique T1036.006 - Enterprise

Archived: 2026-04-05 17:16:28 UTC

Adversaries can hide a program's true filetype by changing the extension of a file. With certain file types (specifically this does not work with .app extensions), appending a space to the end of a filename will change how the file is processed by the operating system.

For example, if there is a Mach-O executable file called `evil.bin`, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to `evil.txt`, then when double clicked by a user, it will launch with the default text editing application (not executing the binary). However, if the file is renamed to `evil.txt ` (note the space at the end), then when double clicked by a user, the true file type is determined by the OS and handled appropriately and the binary will be executed [1].

Adversaries can use this feature to trick users into double clicking benign-looking files of any format and ultimately executing something malicious.

Source: https://attack.mitre.org/techniques/T1036/006