# TTP Detail – T1036.006

## TTP Information

Name: Space after Filename

Description: 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 <code>evil.bin</code>, when it is double clicked by a user, it will launch Terminal.app and execute. If this file is renamed to <code>evil.txt</code>, 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 <code>evil.txt </code> (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 (Citation: Mac Backdoors are back).

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

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Keydnap

## APTs (Intrusion Sets)

* APT38