# TTP Detail – T1036.002

## TTP Information

Name: Right-to-Left Override

Description: Adversaries may abuse the right-to-left override (RTLO or RLO) character (U+202E) to disguise a string and/or file name to make it appear benign. RTLO is a non-printing Unicode character that causes the text that follows it to be displayed in reverse. For example, a Windows screensaver executable named <code>March 25 \u202Excod.scr</code> will display as <code>March 25 rcs.docx</code>. A JavaScript file named <code>photo\_high\_re\u202Egnp.js</code> will be displayed as <code>photo\_high\_resj.png</code>.(Citation: Infosecinstitute RTLO Technique)

Adversaries may abuse the RTLO character as a means of tricking a user into executing what they think is a benign file type. A common use of this technique is with [Spearphishing Attachment](https://attack.mitre.org/techniques/T1566/001)/[Malicious File](https://attack.mitre.org/techniques/T1204/002) since it can trick both end users and defenders if they are not aware of how their tools display and render the RTLO character. Use of the RTLO character has been seen in many targeted intrusion attempts and criminal activity.(Citation: Trend Micro PLEAD RTLO)(Citation: Kaspersky RTLO Cyber Crime) RTLO can be used in the Windows Registry as well, where regedit.exe displays the reversed characters but the command line tool reg.exe does not by default.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## APTs (Intrusion Sets)

* BRONZE BUTLER
* BlackTech
* Ferocious Kitten
* Ke3chang
* Scarlet Mimic