# TTP Detail – T1222.002

## TTP Information

Name: Linux and Mac File and Directory Permissions Modification

Description: Adversaries may modify file or directory permissions/attributes to evade access control lists (ACLs) and access protected files.(Citation: Hybrid Analysis Icacls1 June 2018)(Citation: Hybrid Analysis Icacls2 May 2018) File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL implementations vary by platform, but generally explicitly designate which users or groups can perform which actions (read, write, execute, etc.).

Most Linux and Linux-based platforms provide a standard set of permission groups (user, group, and other) and a standard set of permissions (read, write, and execute) that are applied to each group. While nuances of each platform’s permissions implementation may vary, most of the platforms provide two primary commands used to manipulate file and directory ACLs: <code>chown</code> (short for change owner), and <code>chmod</code> (short for change mode).

Adversarial may use these commands to make themselves the owner of files and directories or change the mode if current permissions allow it. They could subsequently lock others out of the file. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Unix Shell Configuration Modification](https://attack.mitre.org/techniques/T1546/004) or tainting/hijacking other instrumental binary/configuration files via [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574).(Citation: 20 macOS Common Tools and Techniques)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Black Basta
* Bundlore
* COATHANGER
* Dok
* Kinsing
* OSX/Shlayer
* OSX\_OCEANLOTUS.D
* P.A.S. Webshell
* Penquin
* XCSSET

## APTs (Intrusion Sets)

* APT32
* Rocke
* TeamTNT