# TTP Detail – T1222

## TTP Information

Name: 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.).

Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory’s existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories. Specific file and directory modifications may be a required step for many techniques, such as establishing Persistence via [Accessibility Features](https://attack.mitre.org/techniques/T1546/008), [Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037), [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).

Adversaries may also change permissions of symbolic links. For example, malware (particularly ransomware) may modify symbolic links and associated settings to enable access to files from local shortcuts with remote paths.(Citation: new\_rust\_based\_ransomware)(Citation: bad\_luck\_blackcat)(Citation: falconoverwatch\_blackcat\_attack)(Citation: blackmatter\_blackcat)(Citation: fsutil\_behavior)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion