# TTP Detail – T1070.010

## TTP Information

Name: Relocate Malware

Description: Once a payload is delivered, adversaries may reproduce copies of the same malware on the victim system to remove evidence of their presence and/or avoid defenses. Copying malware payloads to new locations may also be combined with [File Deletion](https://attack.mitre.org/techniques/T1070/004) to cleanup older artifacts.

Relocating malware may be a part of many actions intended to evade defenses. For example, adversaries may copy and rename payloads to better blend into the local environment (i.e., [Match Legitimate Resource Name or Location](https://attack.mitre.org/techniques/T1036/005)).(Citation: DFIR Report Trickbot June 2023) Payloads may also be repositioned to target [File/Path Exclusions](https://attack.mitre.org/techniques/T1564/012) as well as specific locations associated with establishing [Persistence](https://attack.mitre.org/tactics/TA0003).(Citation: Latrodectus APR 2024)

Relocating malicious payloads may also hinder defensive analysis, especially to separate these payloads from earlier events (such as [User Execution](https://attack.mitre.org/techniques/T1204) and [Phishing](https://attack.mitre.org/techniques/T1566)) that may have generated alerts or otherwise drawn attention from defenders.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion