Indicator Removal: Relocate Malware, Sub-technique T1070.010 - Enterprise

Archived: 2026-04-05 16:53:45 UTC

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 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).[1] Payloads may also be repositioned to target File/Path Exclusions as well as specific locations associated with establishing Persistence.[2]

Relocating malicious payloads may also hinder defensive analysis, especially to separate these payloads from earlier events (such as User Execution and Phishing) that may have generated alerts or otherwise drawn attention from defenders. Moving payloads into target directories does not alter the Creation timestamp, thereby evading detection logic reliant on modifications to this artifact (i.e., Timestomp).

Source: https://attack.mitre.org/techniques/T1070/010