Hide Artifacts: File/Path Exclusions, Sub-technique T1564.012 - Enterprise

Archived: 2026-04-05 15:01:18 UTC

Adversaries may attempt to hide their file-based artifacts by writing them to specific folders or file names excluded from antivirus (AV) scanning and other defensive capabilities. AV and other file-based scanners often include exclusions to optimize performance as well as ease installation and legitimate use of applications. These exclusions may be contextual (e.g., scans are only initiated in response to specific triggering events/alerts), but are also often hardcoded strings referencing specific folders and/or files assumed to be trusted and legitimate.[1]

Adversaries may abuse these exclusions to hide their file-based artifacts. For example, rather than tampering with tool settings to add a new exclusion (i.e., Disable or Modify Tools), adversaries may drop their file-based payloads in default or otherwise well-known exclusions. Adversaries may also use Security Software Discovery and other Discovery/Reconnaissance activities to both discover and verify existing exclusions in a victim environment.

Source: https://attack.mitre.org/techniques/T1564/012