Hide Artifacts: Bind Mounts, Sub-technique T1564.013 - Enterprise

Archived: 2026-04-05 16:40:35 UTC

Adversaries may abuse bind mounts on file structures to hide their activity and artifacts from native utilities. A bind mount maps a directory or file from one location on the filesystem to another, similar to a shortcut on Windows. It’s commonly used to provide access to specific files or directories across different environments, such as inside containers or chroot environments, and requires sudo access.

Adversaries may use bind mounts to map either an empty directory or a benign `/proc` directory to a malicious process’s `/proc` directory. Using the commands `mount -o bind /proc/benign-process /proc/malicious-process` (or `mount -B`), the malicious process's `/proc` directory is overlayed with the contents of a benign process's `/proc` directory. When system utilities query process activity, such as `ps` and `top`, the kernel follows the bind mount and presents the benign directory’s contents instead of the malicious process's actual `/proc` directory. As a result, these utilities display information that appears to come from the benign process, effectively hiding the malicious process's metadata, executable, or other artifacts from detection.[1][2]

Source: https://attack.mitre.org/techniques/T1564/013