Masquerading, Technique T0849 - ICS

Archived: 2026-04-05 16:41:53 UTC

Adversaries may use masquerading to disguise a malicious application or executable as another file, to avoid operator and engineer suspicion. Possible disguises of these masquerading files can include commonly found programs, expected vendor executables and configuration files, and other commonplace application and naming conventions. By impersonating expected and vendor-relevant files and applications, operators and engineers may not notice the presence of the underlying malicious content and possibly end up running those masquerading as legitimate functions.

Applications and other files commonly found on Windows systems or in engineering workstations have been impersonated before. This can be as simple as renaming a file to effectively disguise it in the ICS environment.

Source: https://attack.mitre.org/techniques/T0849