Project File Infection, Technique T0873 - ICS

Archived: 2026-04-05 17:07:59 UTC

Adversaries may attempt to infect project files with malicious code. These project files may consist of objects, program organization units, variables such as tags, documentation, and other configurations needed for PLC programs to function. [1] Using built in functions of the engineering software, adversaries may be able to download an infected program to a PLC in the operating environment enabling further Execution and Persistence techniques. [2]

Adversaries may export their own code into project files with conditions to execute at specific intervals. [3] Malicious programs allow adversaries control of all aspects of the process enabled by the PLC. Once the project file is downloaded to a PLC the workstation device may be disconnected with the infected project file still executing. [2]

Source: https://attack.mitre.org/techniques/T0873