

Engineering Workstation Compromise, Technique T0818 - ICS

Archived: 2026-04-05 14:59:48 UTC

Adversaries will compromise and gain control of an engineering workstation for Initial Access into the control system environment. Access to an engineering workstation may occur through or physical means, such as a Valid Accounts with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks. An Engineering Workstation is designed as a reliable computing platform that configures, maintains, and diagnoses control system equipment and applications. Compromise of an engineering workstation may provide access to, and control of, other control system applications and equipment. In the Maroochy attack, the adversary utilized a computer, possibly stolen, with proprietary engineering software to communicate with a wastewater system.

Source: <https://attack.mitre.org/techniques/T0818>