Lateral Movement, Tactic TA0109 - ICS

Archived: 2026-04-05 14:33:24 UTC

The adversary is trying to move through your ICS environment.

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. These techniques abuse default credentials, known accounts, and vulnerable services, and may also leverage dual-homed devices and systems that reside on both the IT and OT networks. The adversary uses these techniques to pivot to their next point in the environment, positioning themselves to where they want to be or think they should be. Following through on their primary objective often requires Discovery of the network and Collection to develop awareness of unique ICS devices and processes, in order to find their target and subsequently gain access to it. Reaching this objective often involves pivoting through multiple systems, devices, and accounts. Adversaries may install their own remote tools to accomplish Lateral Movement or leverage default tools, programs, and manufacturer set or other legitimate credentials native to the network, which may be stealthier.

Source: https://attack.mitre.org/tactics/TA0109