Command and Control, Tactic TA0101 - ICS

Archived: 2026-04-05 13:55:48 UTC

The adversary is trying to communicate with and control compromised systems, controllers, and platforms with access to your ICS environment.

Command and Control consists of techniques that adversaries use to communicate with and send commands to compromised systems, devices, controllers, and platforms with specialized applications used in ICS environments. Examples of these specialized communication devices include human machine interfaces (HMIs), data historians, SCADA servers, and engineering workstations (EWS). Adversaries often seek to use commonly available resources and mimic expected network traffic to avoid detection and suspicion. For instance, commonly used ports and protocols in ICS environments, and even expected IT resources, depending on the target network. Command and Control may be established to varying degrees of stealth, often depending on the victim’s network structure and defenses.

Source: https://attack.mitre.org/tactics/TA0101