Collection, Tactic TA0100 - ICS

Archived: 2026-04-05 14:47:53 UTC

The adversary is trying to gather data of interest and domain knowledge on your ICS environment to inform their goal.

Collection consists of techniques adversaries use to gather domain knowledge and obtain contextual feedback in an ICS environment. This tactic is often performed as part of Discovery, to compile data on control systems and targets of interest that may be used to follow through on the adversary's objective. Examples of these techniques include observing operation states, capturing screenshots, identifying unique device roles, and gathering system and diagram schematics. Collection of this data can play a key role in planning, executing, and even revising an ICS-targeted attack. Methods of collection depend on the categories of data being targeted, which can include protocol specific, device specific, and process specific configurations and functionality. Information collected may pertain to a combination of system, supervisory, device, and network related data, which conceptually fall under high, medium, and low levels of plan operations. For example, information repositories on plant data at a high level or device specific programs at a low level. Sensitive floor plans, vendor device manuals, and other references may also be at risk and exposed on the internet or otherwise publicly accessible.

Source: https://attack.mitre.org/tactics/TA0100