Transient Cyber Asset, Technique T0864 - ICS

Archived: 2026-04-05 18:28:28 UTC

Adversaries may target devices that are transient across ICS networks and external networks. Normally, transient assets are brought into an environment by authorized personnel and do not remain in that environment on a permanent basis. [1] Transient assets are commonly needed to support management functions and may be more common in systems where a remotely managed asset is not feasible, external connections for remote access do not exist, or 3rd party contractor/vendor access is required.

Adversaries may take advantage of transient assets in different ways. For instance, adversaries may target a transient asset when it is connected to an external network and then leverage its trusted access in another environment to launch an attack. They may also take advantage of installed applications and libraries that are used by legitimate end-users to interact with control system devices.

Transient assets, in some cases, may not be deployed with a secure configuration leading to weaknesses that could allow an adversary to propagate malicious executable code, e.g., the transient asset may be infected by malware and when connected to an ICS environment the malware propagates onto other systems.
