Valid Accounts, Technique T0859 - ICS

Archived: 2026-04-05 13:29:30 UTC

Adversaries may steal the credentials of a specific user or service account using credential access techniques. In some cases, default credentials for control system devices may be publicly available. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network, and may even be used for persistent access to remote systems. Compromised and default credentials may also grant an adversary increased privilege to specific systems and devices or access to restricted areas of the network. Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way.

Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence. [1]

The overlap of credentials and permissions across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) and possibly between the enterprise and operational technology environments. Adversaries may be able to leverage valid credentials from one system to gain access to another system.

Source: https://attack.mitre.org/techniques/T0859