Block Command Message, Technique T0803 - ICS

Archived: 2026-04-05 18:22:24 UTC

Adversaries may block a command message from reaching its intended target to prevent command execution. In OT networks, command messages are sent to provide instructions to control system devices. A blocked command message can inhibit response functions from correcting a disruption or unsafe condition. [1] [2]

Sub-techniques: No sub-techniques

Last Modified: 15 April 2025

Procedure Examples

Targeted Assets

ID	Asset
A0007	Control Server
A0017	Distributed Control System (DCS) Controller
A0013	Field I/O
A0002	Human-Machine Interface (HMI)
A0005	Intelligent Electronic Device (IED)
A0018	Programmable Automation Controller (PAC)
A0003	Programmable Logic Controller (PLC)
A0004	Remote Terminal Unit (RTU)
A0010	Safety Controller

Mitigations

ID	Mitigation	Description
M0807	Network Allowlists	Utilize network allowlists to restrict unnecessary connections to network devices (e.g., comm servers, serial to ethernet converters) and services, especially in cases when devices have limits on the number of simultaneous sessions they support.

ID	Mitigation	Description
M0810	Out-of-Band Communications Channel	Provide an alternative method for sending critical commands message to outstations, this could include using radio/cell communication to send messages to a field technician that physically performs the control function.
M0814	Static Network Configuration	Unauthorized connections can be prevented by statically defining the hosts and ports used for automation protocol connections.

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0784	Detection of Block Command Message	AN1916	Monitor for the termination of processes or services associated with ICS automation protocols and application software which could help detect blocked communications. Monitor for lack of operational process data which may help identify a loss of communications. This will not directly detect the technique's execution, but instead may provide additional evidence that the technique has been used and may complement other detections. Monitor application logs for changes to settings and other events associated with network protocols that may be used to block communications. Monitor for a loss of network communications, which may indicate this technique is being used. Monitor asset alarms which may help identify a loss of communications. Consider correlating alarms with other data sources that indicate traffic has been blocked, such as network traffic. In cases where alternative methods of communicating with outstations exist alarms may still be visible even if command messages are blocked.

References

1. Bonnie Zhu, Anthony Joseph, Shankar Sastry 2011 A Taxonomy of Cyber Attacks on SCADA Systems Retrieved. 2018/01/12

2. Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems 2016, March 18 Analysis of the Cyber Attack on the Ukranian Power Grid: Defense Use Case Retrieved. 2018/03/27

3. Electricity Information Sharing and Analysis Center; SANS Industrial Control Systems. (2016, March 18). Analysis of the Cyber Attack on the Ukranian Power Grid: Defense Use Case. Retrieved March 27, 2018.
4. Anton Cherepanov, ESET 2017, June 12 Win32/Industroyer: A new threat for industrial control systems Retrieved. 2017/09/15
