# TTP Detail – T1059.008

## TTP Information

Name: Network Device CLI

Description: Adversaries may abuse scripting or built-in command line interpreters (CLI) on network devices to execute malicious command and payloads. The CLI is the primary means through which users and administrators interact with the device in order to view system information, modify device operations, or perform diagnostic and administrative functions. CLIs typically contain various permission levels required for different commands.

Scripting interpreters automate tasks and extend functionality beyond the command set included in the network OS. The CLI and scripting interpreter are accessible through a direct console connection, or through remote means, such as telnet or [SSH](https://attack.mitre.org/techniques/T1021/004).

Adversaries can use the network CLI to change how network devices behave and operate. The CLI may be used to manipulate traffic flows to intercept or manipulate data, modify startup configuration parameters to load malicious system software, or to disable security features or logging to avoid detection.(Citation: Cisco Synful Knock Evolution)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Line Dancer