# TTP Detail – T1602.002

## TTP Information

Name: Network Device Configuration Dump

Description: Adversaries may access network configuration files to collect sensitive data about the device and the network. The network configuration is a file containing parameters that determine the operation of the device. The device typically stores an in-memory copy of the configuration while operating, and a separate configuration on non-volatile storage to load after device reset. Adversaries can inspect the configuration files to reveal information about the target network and its layout, the network device and its software, or identifying legitimate accounts and credentials for later use.

Adversaries can use common management tools and protocols, such as Simple Network Management Protocol (SNMP) and Smart Install (SMI), to access network configuration files.(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)(Citation: Cisco Blog Legacy Device Attacks) These tools may be used to query specific data from a configuration repository or configure the device to export the configuration for later analysis.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## APTs (Intrusion Sets)

* Salt Typhoon