# TTP Detail – T1219.003

## TTP Information

Name: Remote Access Hardware

Description: An adversary may use legitimate remote access hardware to establish an interactive command and control channel to target systems within networks. These services, including IP-based keyboard, video, or mouse (KVM) devices such as TinyPilot and PiKVM, are commonly used as legitimate tools and may be allowed by peripheral device policies within a target environment.

Remote access hardware may be physically installed and used post-compromise as an alternate communications channel for redundant access or as a way to establish an interactive remote session with the target system. Using hardware-based remote access tools may allow threat actors to bypass software security solutions and gain more control over the compromised device(s).(Citation: Palo Alto Unit 42 North Korean IT Workers 2024)(Citation: Google Cloud Threat Intelligence DPRK IT Workers 2024)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control