# TTP Detail – T1059.012

## TTP Information

Name: Hypervisor CLI

Description: Adversaries may abuse hypervisor command line interpreters (CLIs) to execute malicious commands. Hypervisor CLIs typically enable a wide variety of functionality for managing both the hypervisor itself and the guest virtual machines it hosts.

For example, on ESXi systems, tools such as `esxcli` and `vim-cmd` allow administrators to configure firewall rules and log forwarding on the hypervisor, list virtual machines, start and stop virtual machines, and more.(Citation: Broadcom ESXCLI Reference)(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)(Citation: LOLESXi) Adversaries may be able to leverage these tools in order to support further actions, such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Cheerscrypt
* Royal