# TTP Detail – T1675

## TTP Information

Name: ESXi Administration Command

Description: Adversaries may abuse ESXi administration services to execute commands on guest machines hosted within an ESXi virtual environment. Persistent background services on ESXi-hosted VMs, such as the VMware Tools Daemon Service, allow for remote management from the ESXi server. The tools daemon service runs as `vmtoolsd.exe` on Windows guest operating systems, `vmware-tools-daemon` on macOS, and `vmtoolsd ` on Linux.(Citation: Broadcom VMware Tools Services)

Adversaries may leverage a variety of tools to execute commands on ESXi-hosted VMs – for example, by using the vSphere Web Services SDK to programmatically execute commands and scripts via APIs such as `StartProgramInGuest`, `ListProcessesInGuest`, `ListFileInGuest`, and `InitiateFileTransferFromGuest`.(Citation: Google Cloud Threat Intelligence VMWare ESXi Zero-Day 2023)(Citation: Broadcom Running Guest OS Operations) This may enable follow-on behaviors on the guest VMs, such as [File and Directory Discovery](https://attack.mitre.org/techniques/T1083), [Data from Local System](https://attack.mitre.org/techniques/T1005), or [OS Credential Dumping](https://attack.mitre.org/techniques/T1003).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution