# TTP Detail – T1673

## TTP Information

Name: Virtual Machine Discovery

Description: An adversary may attempt to enumerate running virtual machines (VMs) after gaining access to a host or hypervisor. For example, adversaries may enumerate a list of VMs on an ESXi hypervisor using a [Hypervisor CLI](https://attack.mitre.org/techniques/T1059/012) such as `esxcli` or `vim-cmd` (e.g. `esxcli vm process list or vim-cmd vmsvc/getallvms`).(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)(Citation: TrendMicro Play) Adversaries may also directly leverage a graphical user interface, such as VMware vCenter, in order to view virtual machines on a host.

Adversaries may use the information from [Virtual Machine Discovery](https://attack.mitre.org/techniques/T1673) during discovery to shape follow-on behaviors. Subsequently discovered VMs may be leveraged for follow-on activities such as [Service Stop](https://attack.mitre.org/techniques/T1489) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Cheerscrypt